Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of)
)
Wireless Telecommunications Bureau and)
Office of Engineering and Technology) GN Docket No. 15-319
Establish Procedure and Deadline for Filing)
Spectrum Access System (SAS))
Administrator(s) and Environmental Sensing)
Capability (ESC) Operator(s) Applications

Proposal by RED Technologies for Spectrum Access System Administrator

Version: 1.0

Date: 05/05/2017

Pierre-Jean Muller
Chief Executive Officer
RED Technologies
130, rue de Lourmel
75015 Paris – France

EXECUTIVE SUMMARY

RED Technologies, a leading developer of innovative spectrum management, is a French SME born from the innovation spectrum scarcity triggers. Today, our award-winning company, whose focus is dynamic spectrum management, is the premier enabler of Licensed Shared Access (LSA) with its LSAlive© cloud-based solution, already piloted with global telecoms players across two major European terrains.

RED Technologies has been deeply involved in the regulation framework changes that enabled LSA and has patented inventions related to facilitating their success. Through our engagement with the ECC and CEPT, we follow and influence spectrum sharing policy and we are leading LSA standardization activities at ETSI and 3GPP. It is from this pivotal position that we now seek to invest in the US by becoming a SAS Administrator through our SASlive© solution, the focus of this proposal.

RED Technologies' comprises a team of seasoned global telecoms professionals flanked by an influential Board, who together bring deep and unique expertise and experience to the administration of SAS in the United States. Our proficiency in the design and delivery of LSA has served as a test-bed and a springboard for our fully functional United States SASlive© solution. This robust product offers a secure SAS infrastructure housed in the cloud and an advanced request management process, managed by a secure web portal that addresses all FCC requirements and operates a high quality of service based on stringent key performance indicators.

Investing in the US, a country so profoundly linked to telecoms innovation and entrepreneurship, is RED Technologies' paramount focus today. It is our intention to contribute to US job creation, to innovation and to the narrowing of digital divides by providing a locally delivered, state-of-the art, secure and rapid spectrum management service. To this effect, we are opening a SAS service center in Arlington, Virginia supported by a trained, locally recruited team. We expect to see fruitful idea exchange across our European and US team members, partners and customer base as we evolve our SAS and LSA solutions in parallel.

Our intention is to expand our offer in the US as part of a business strategy that reaches far beyond Europe and we bring robust, tested technology and the force of a dynamic, global-minded and skilled team to this task. We also offer a unique stance on spectrum management innovation through our knowledge of LSA and the European ecosystem which, we believe, will serve to stimulate entrepreneurship and trigger creative thinking within the sector.

Content

Figures

Tables

1. DOCUMENT PURPOSE

The Wireless Telecommunications Bureau and the Office of Engineering and Technology seek proposals for future Spectrum Access System Administrator(s) and Environmental Sensing Capability operator(s) in the 3550-3700 MHz band (3.5 GHz Band). See Public Notice ([Ref. 01], [Ref. 03]).

This document is the response from RED Technologies for managing the Spectrum Access System (SAS).

Managing of the Environmental Sensing Capability (ESC) is out of the scope of this document.

Note:

> *Unlike the SAS-SAS and SAS-CBSD interfaces, the SAS-ESC interface is not standardized. RED Technologies will adapt its SAS-ESC interface according to the specifications of the ESC system to which its SAS will be connected.*
>
> *Thanks to a modular and adaptable architecture of its SAS (see §5.2) these adaptations can be realized quickly. Moreover, the ESC-SAS protocol will be designed to consider the security requirement as per the FCC's rules (see documents [Ref. 04] and [Ref. 05]).*
>
> ***In addition, RED Technologies is in contact with prospective ESC operators and together with them will collaborate in defining a fully functional and secured SAS-ESC interface** (see §5.2.1.4.4.3).*
>
> *If the SAS is deployed before the partner ESC, and until this ESC becomes operational, the SAS Administrator will enforce exclusion zones as per the FCC's rules (see documents [Ref. 04] and [Ref. 05]) and will prohibit CBSDs in those zones.*
>
> *Once a partner ESC has become operational in an exclusion zone, this zone will no longer be considered as a permanent exclusion zone by the SAS Administrator. The SAS Administrator will comply with the information provided by the partner ESC to authorize the CBSD to transmit in this zone.*

This Application is organized as follows:

- Section 2 describes RED Technologies compliance with FCC and WInnF requirements,
- Section 3 reminds the 3.5 GHZ CBRS band concepts and objectives,
- Section 4 presents RED Technologies along with its technical and financial capabilities,
- Section 5 provides details about RED Technologies' SAS administration and product,
- Section 6 provides appendix.

2. FCC & WINNF COMPLIANCE

2.1. Compliance with FCC

2.1.1. FCC rules Part 96 Affirmation

RED Technologies affirms that its SAS will comply with all applicable rules as well as applicable enforcement mechanisms and procedures:

- **Subpart A – GENERAL RULES**
  - *96.7 – Authorization Required*
  - *96.11 – Frequencies*
  - *96.13 – Frequency Assignments*

- **Subpart B – INCUMBENT PROTECTION**
  - *96.15 – Protection of Federal Incumbent Users*

- **Subpart C - PRIORITY ACCESS**
  - *96.17 - Protection of Existing FSS Earth Stations in the 3600-3650 MHz Band and 3700-4200 MHz Band*
  - **96.19 –Operation Near Canadian and Mexican Borders**
  - *96.21 – Protection of Existing Operators in the 3650-3700 MHz Band*
  - *96.23 – Authorization*
  - *96.25 – Priority Access Licenses*
  - *96.31 – Aggregation of Priority Access Licenses*

- **Subpart D - GENERAL AUTHORIZED ACCESS**
  - *96.33 –Authorization*
  - *96.35 – General Authorized Access Use*

- **Subpart E - TECHNICAL RULES**
  - *96.39 - Citizens Broadband Radio Service Device (CBSD) General Requirements*
  - *96.41 – General Radio Requirements*
  - *96.43 – Additional Requirements for Category A CBSDs*
  - *96.45 - Additional Requirements for Category B CBSDs*

- **Subpart F – SPECTRUM ACCESS SYSTEM**
  - **96.53 - Spectrum access system purposes and functionality**
  - **96.55 - Information gathering and retention**
  - **96.57 - Registration, authentication, and authorization of Citizens Broadband Radio Service Devices**
  - **96.59 - Frequency assignment**
  - **96.61 –Security**

- **96.63 –Spectrum Access System Administrators**
- **96.65 –Spectrum Access System Administrator Fees**
- **96.66 –Spectrum Access System Responsibilities Related to Priority Access Spectrum Manager Leases**

- **Subpart G – ENVIRONMENTAL SENSING CAPABILITY**
  - *96.67 – Environmental Sensing Capability*

Note:

Rules marked in bold are specific to SAS Administrators.

Rules marked in italic contain some SAS Administrators requirements but not only.

2.1.2. FCC Public Notice compliance matrix

The table below lists requirements coming from the FCC Public Notice document ([Ref. 01], section IV) and refers to the paragraphs of this document that meet these requirements.

	Requirement Description	Reference	Comment
General requirements			
1	A detailed description of the scope of the functions that the SAS and/or ESC would perform	3.2.5 5.2.1.4	For SAS only
2	A demonstration that the prospective SAS Administrator or ESC operator possesses sufficient technical expertise to operate an SAS and/or ESC, including the qualifications of key personnel who will be responsible for operating and maintaining the SAS and/or ESC.	2.3 4.4 5.1.1.3	For SAS only
3	The prospective SAS Administrator or ESC operator must demonstrate that it is financially capable of operating an SAS and/or ESC for a five-year term. The proposal must include a description of the prospective SAS Administrator or ESC operator's business structure including ownership information. To the extent that the proponent will rely on fees to support its operations, the proposal should also describe the fee collection process and the entities from which the fees will be collected.	4.5 4.1.4 4.2	For SAS only
4	A description of how data will be securely communicated between the SAS and its associated ESC and how quickly and reliably these communications will be accomplished.	3.2.6 5.2.1.4.4.3	For SAS only
5	Technical diagrams showing the architecture of the SAS and/or ESC and a detailed description of how each function operates and how each function interacts with the other functions.	5.2.1	For SAS only
6	A description of the propagation model and any other assumptions that the prospective SAS Administrator or ESC operator proposes to use to model operations and facilitate coordination in the band.	5.2.1.4.1 5.2.1.4.3.2	For SAS only
7	A description of the methods that will be used: - to update software and firmware and - to expeditiously identify and address security vulnerabilities.	5.1.3.2 5.2.1.2.2 5.2.1.4.2.2 5.2.5.3	For SAS only

8	An affirmation that the prospective SAS Administrator and/or ESC operator (and its respective SAS and/or ESC) will comply - with all of the applicable rules - as well as applicable enforcement mechanisms and procedures	2.1.1	For SAS only
Specific SAS requirements			
1	A detailed description of how the SAS will retain, secure, and verify information from CBSDs (including location data), licensees, associated ESCs, and other SASs.	5.2.1.4.2 5.2.1.4.3.1 5.2.1.4.4.1 5.2.1.4.4.2 5.2.1.4.4.3	
2	A demonstration that the SAS will be capable of resolving various sources of interference between and among Citizens Broadband Radio Service users and/or Incumbent users.	5.2.1.4.3.2 5.2.1.4.3.4	
3	A description of how the SAS will ensure that non-federal FSS earth stations and grandfathered 3650-3700 MHz licensees are protected from harmful interference consistent with the rules	5.2.1.4.3.2 5.2.1.4.3.4	
4	A description of how coordination will be effectuated (e.g., through data synchronization) between multiple SASs, if multiple SASs are authorized, and how quickly this synchronization of data will be accomplished.	5.2.1.4.4.2	
5	If the prospective SAS Administrator will not be performing all SAS functions, it must provide information on the entities operating other functions and the relationship between itself and these other entities. In particular, it must address how the Commission can ensure that all of the requirements for SAS Administrators in Part 96, subpart F are satisfied when SAS functions are divided among multiple entities, including a description of how data will be transferred among these various related entities and SASs, if multiple SASs are authorized, and the expected schedule of such data transfers (i.e., real-time, once an hour, etc.).	2.1.1	All Requirement of SAS Administrators in Part 96, subpart F are supported by RED Technologies SASlive©
6	A description of the methods (e.g., interfaces, protocols) that will be used by: CBSDs to communicate with the SAS; the SAS to communicate with CBSDs; the SAS to communicate with other SASs; and, if applicable, the SAS to communicate with one or more ESCs. The prospective SAS Administrator must also describe the procedures, if any, which it plans to use to verify that a CBSD can properly communicate with the SAS	5.2.1.4.4	
7	An affirmation that, consistent with section 96.55 of the Commission's rules, the SAS will only retain records and information or instructions received regarding federal transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process	2.1.1 5.2.1.4.2.2	
8	A description of the security methods that the prospective SAS Administrator plans to use to ensure that unauthorized parties cannot access or alter the SAS or otherwise corrupt the operation of the SAS in performing its intended functions, consistent with the Commission's rules.	5.2.1.2.2 5.2.5.3 5.2.1.4.4 5.1.2.1 5.1.2.2	

9	Descriptions of dynamic workflow scenarios for how the SAS will manage and assign spectrum resources to ensure that geographically and spectrally adjacent operations are coordinated consistent with the Commission's rules. Use case scenarios should include the methodology and protection approach for cases of radio interference due to adjacent blocking, out-of-band emissions, and aggregate co-channel interference. Describe how multiple SASs will coordinate the calculation of aggregate interference for protecting incumbent users and Priority Access licensees.	5.2.1.4.3.2 5.2.1.4.3.4	
10	A description of the methods that the SAS will use to make information stored or retained by the SAS available in response to a request from authorized Commission personnel.	5.1.2	

Table 1: FCC Public Notice compliance matrix

2.2. COMPLIANCE WITH WINNF

RED Technologies affirms that its SAS will comply with all WInnF requirements defined by the Release 1 documents; and in particular, those referred in section §6.1.

Furthermore, RED Technologies, as an active member of the WinnF, plays a contributor role in continuous development of 3.5 GHz CBRS standards and tests. Given this, we expect our SAS product team to continuously update the product with new requirements and provide our customers and other beneficiaries of our SAS solution with latest CBRS releases.

2.3. STAFF RESPONSIBLE FOR COMPLIANCE

RED Technologies designates Luc DAVIT, senior manager at RED Technologies, to ensure compliance with the rules set forth by the Commission.

2.4. RED TECHNOLOGIES' TRACEABILITY COMPLIANCE PROCESS

Compliance with the requirements from the FCC and the WInnF is implemented thanks to a "Traceability Process" based on:

- A **Document Tree** that defines the FCC and the WInnF documents / versions applicable to a SAS software release,
- A **Compliance Matrix** that traces which applicable requirements are covered by a SAS software release and its corresponding set of tests,
- A **Test Report** that gives the test coverage of the requirements and the test status for a SAS software release.

Relations between these different documents are described below:

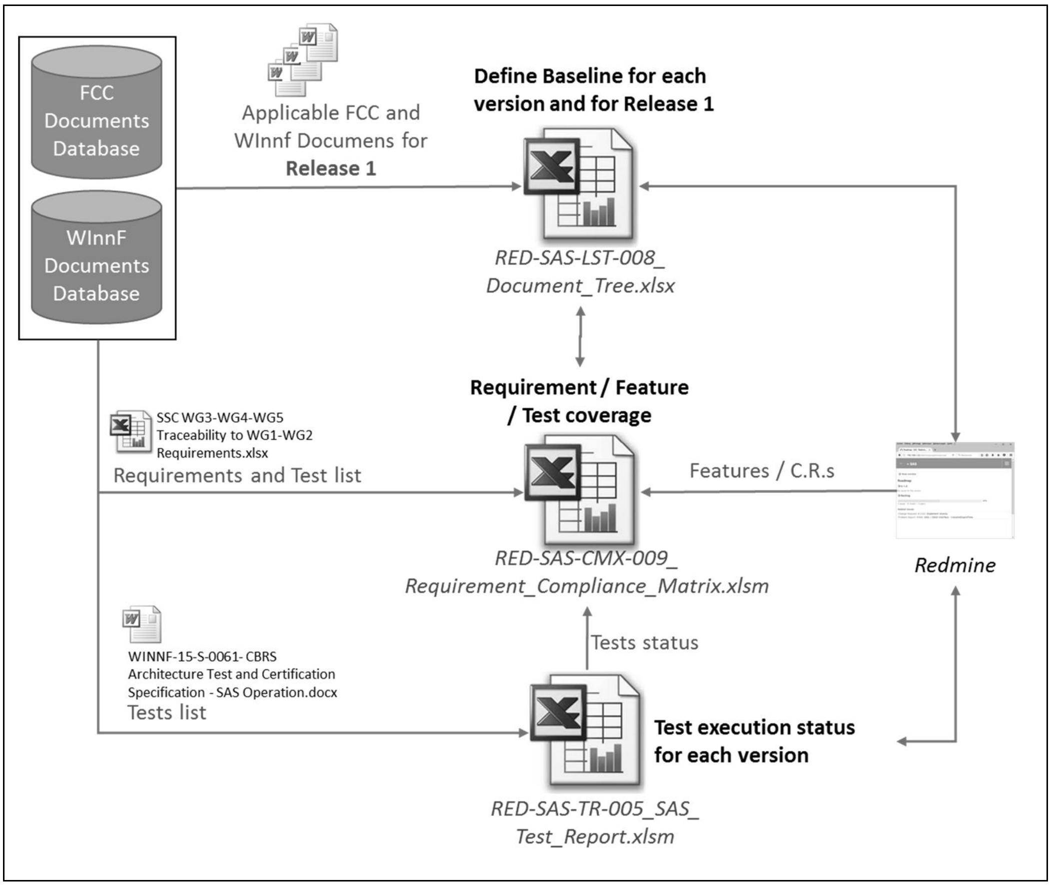

FCC Documents Database
WInnF Documents Database
Applicable FCC and WInnf Documens for Release 1
Define Baseline for each version and for Release 1
RED-SAS-LST-008_ Document_Tree.xlsx
Requirement / Feature / Test coverage
SSC WG3-WG4-WG5 Traceability to WG1-WG2 Requirements.xlsx
Requirements and Test list
Features / C.R.s
Redmine
RED-SAS-CMX-009_ Requirement_Compliance_Matrix.xlsm
Tests status
WINNF-15-S-0061- CBRS Architecture Test and Certification Specification - SAS Operation.docx
Tests list
Test execution status for each version
RED-SAS-TR-005_SAS_ Test_Report.xlsm

Figure 1 : Traceability Process

3. FCC' 3.5 GHZ CBRS BAND

3.1. A THREE-TIERED ACCESS MODEL

Historically, the 3550-3700 MHz (3.5 GHz) band was reserved for the Department of Defense (DoD) for radar systems but also for Fixed Satellite Service (FSS). The Federal Communications Commission decided to open this band to new actors and so created the **Citizens Broadband Radio Service (CBRS)**.

To do this, a three-tiered access model has been identified:

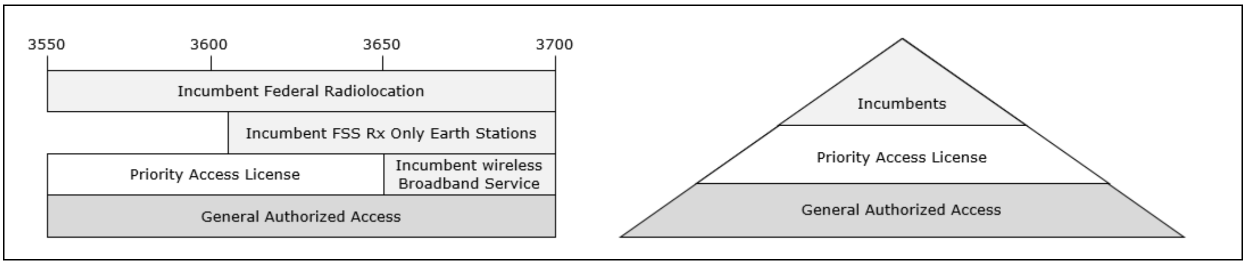

3550
3600
3650
3700
Incumbent Federal Radiolocation
Incumbent FSS Rx Only Earth Stations
Priority Access License
Incumbent wireless Broadband Service
General Authorized Access
Incumbents
Priority Access License
General Authorized Access

Figure 2 Three-Tier Model

This model defines the rules for spectrum sharing between the different actors who have been split into three main categories:

- Incumbent Users:
    - Authorized Federal entities, Fixed Satellite Service (FSS) operators, or Grandfathered Wireless Broadband Licensees. These users have absolute protection from interference from other users.
- Priority Access Licensee Users:
    - Users who hold one or more Priority Access License (PAL). These users shall be protected from interference from other PALS and General Authorized Access users.
- General Authorized Access (GAA) Users:
    - Users who are not be subject to individually-issued licenses and shall not cause interference to higher level users (Incumbent & PAL).

To manage the rules of this spectrum sharing model a 3.5 GHz CBRS band system has been defined by the FCC (see [Ref. 04])

3.2. 3.5 GHz CBRS band system Overview

The 3.5 GHz CBRS band system is composed of a set of functional entities linked together as shown in the diagram below:

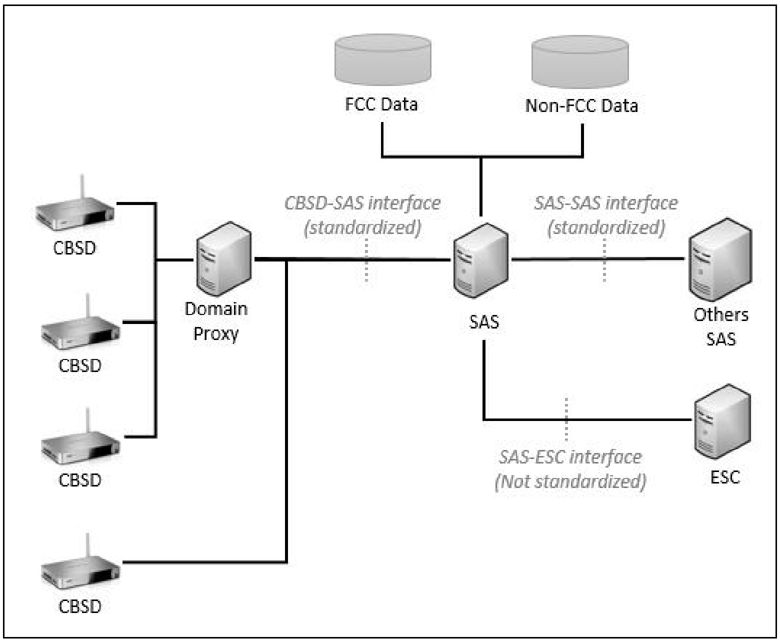


Figure 3 3.5 GHz CBRS band system overview

3.2.1. CBSD

Citizens Broadband Radio Service Device (CBSD) are fixed stations, or sets of fixed stations, that operate on a Priority Access or General Authorized Access.

For CBSDs' that comprise multiple nodes or networks of nodes, CBSD requirements apply to each node even if network management and communication with the SAS is accomplished via a single network interface.

3.2.2. Domain Proxy

The Domain Proxy is an intermediate device between the CBSDs and the SAS. On the one hand, it synchronizes and aggregates messages sent from the CBSDs to the SAS, and on the other hand, it desegregates and roots messages sent from the SAS to the corresponding CBSDs.

3.2.3. FCC Data

The FCC provides a set of data for the 3.5 GHz CBRS band needs and in particular for:

- FSS sites,
- Grandfathered Wireless Broadband Licensees protection zones,
- FCC IDs for CBSDs,
- PAL licenses.

This data can be retrieved from the FCC web portal.

3.2.4. Non-FCC Data

Additional non-FCC data that is also required:

- Census tracks,
- Maritime and terrestrial borders,
- Exclusion zone boundaries (while Environmental Sensing Capability (ESC) are not operational).

This data is provided either by the United States Census Bureau or by the National Telecommunication and Information Administration (NTIA) using their web portal.

Other data such as:

- Shared PAL data (see [Ref. 13]),
- CPI credentials,
- Blacklisted CBSDs,
- Leasing agreement (secondary market),

are either provided by the WInnF or by other organizations

3.2.5. SAS

The SAS is the entity of the 3.5 GHz CBRS band system which authorizes and manages the use of spectrum in the 3550-3700 MHz (3.5 GHz) band. Its main goal is to protect the actors from interference according the rules defined by the Three-Tier Model.

Its main functions as defined in the documents [Ref. 04] and [Ref. 05] are to:

- Determine the available frequencies at a given geographic location and assign them to CBSDs,
- Determine the maximum permissible transmission power level for CBSDs at a given location and communicate that information to the CBSDs,
- Register and authenticate the identification information and location of CBSDs,
- Enforce Exclusion and Protection Zones, including any future changes to such zones, to ensure compatibility between Citizens Broadband Radio Service users and incumbent federal operations,
- Communicate with the ESC and ensure that CBSDs operate in a manner that does not interfere with federal users,
- Ensure that CBSDs protect non-federal incumbent users consistent with the rules,
- Protect Priority Access Licensees from impermissible interference from other Citizens Broadband Radio Service users,
- Facilitate coordination between GAA users to promote a stable spectral environment,
- Ensure secure and reliable transmission of information between the SAS, ESC, and CBSD,
- Provide an approved ESC with any sensing information reported by CBSDs if available,
- Protect Grandfathered Wireless Broadband Licensees until the end of the grandfather period,
- Facilitate coordination and information exchange between SASs.

The SAS shall be operated according to the rules and procedures defined in section 96.63 of the document [Ref. 04]. The entity that administers the SAS is called the **SAS Administrator.**

3.2.6. **ESC**

The Environmental Sensing Capability (ESC) is the system that detects and communicates the presence of a signal from federal incumbent actors to the SAS to facilitate shared spectrum access consistent with sections 96.15 and 96.67 of the document [Ref. 04].

Note:

Unlike the SAS-SAS and SAS-CBSD interfaces, the SAS-ESC interface is not standardized. RED Technologies will adapt its SAS-ESC interface according to the specifications of the ESC system to which its SAS will be connected.

Thanks to the modular and adaptable architecture of its SAS (see §5.2) these adaptations can be realized quickly. Moreover, the ESC-SAS protocol will be designed to consider the security requirement as per the FCC's rules (see documents [Ref. 04] and [Ref. 05]).

In addition, RED Technologies is in contact with prospective ESC operators and together with them will collaborate in defining a fully functional and secured SAS-ESC interface (see §5.2.1.4.4.3).

If the SAS is deployed before the partner ESC, and until this ESC becomes operational, the SAS Administrator will enforce exclusion zones as per the FCC's rules (see documents [Ref. 04] and [Ref. 05]) and will prohibit CBSDs in those zones.

Once a partner ESC has become operational in an exclusion zone, this zone will no longer be considered as a permanent exclusion zone by the SAS Administrator. The SAS Administrator will comply with the information provided by the partner ESC to authorize the CBSD to transmit in this zone.

4. ABOUT RED TECHNOLOGIES

4.1. RED TECHNOLOGIES, FRANCE

4.1.1. Presentation

As telecoms markets move towards 5G and in the face of current and predicted spectrum shortages and increasing demand for accessible and affordable services, policy-makers and industry stakeholders have devised ground-breaking regulatory frameworks called Licensed Shared Access (LSA) in Europe and Citizens Broadband Radio Service (CBRS) in the United States to allow incumbent operators and new entrants to optimize and monetize existing spectrum.

RED Technologies (http://www.redtechnologies.fr/) a leading developer of innovative spectrum management, **was born in 2012** from these new ground-breaking regulatory frameworks (see §4.2)

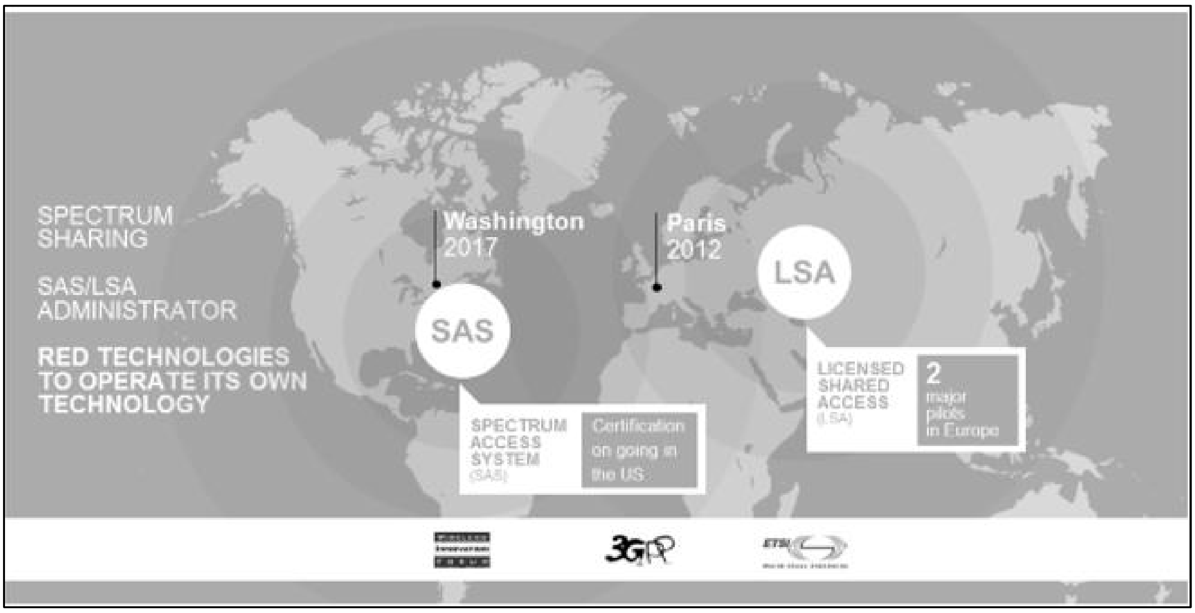

SPECTRUM SHARING
SAS/LSA ADMINISTRATOR
RED TECHNOLOGIES TO OPERATE ITS OWN TECHNOLOGY
Washington 2017
Paris 2012
SAS
LSA
SPECTRUM ACCESS SYSTEM (SAS)
Certification on going in the US
LICENSED SHARED ACCESS (LSA)
2 major pilots in Europe
3GPP
ETSI

Figure 4: RED Technologies locations

RED Technologies' LSAlive© (see §4.3.1, §6.3.1) **and SASlive©** (see §4.3.2, §6.3.2) products use the company's award-winning real time Radio Environment Map (REM) innovation to allow incumbent operators and new entrants to evaluate and plan spectrum shared deployments, localize zones for spectrum sharing geographically and minimize the likelihood of interference between the incumbent and the new entrants' networks. The incumbent's network is protected in a number of ways through standardized information elements, well-defined interfaces and secure access protocols.

RED Technologies received the prestigious Business France, Best Telecom Innovation Award at Mobile World Congress in 2015 (MWC) - https://www.linkedin.com/pulse/mwc15-red-technologies-receives-best-telecom-award-2015-abitbol?trk=pulse-det-nav_art.

RED Technologies is full member of ETSI, 3GPP and the Wireless Innovation Forum and is an active contributor to European regulatory bodies ECC and CEPT. RED Technologies leads LSA standards development in 3GPP and in ETSI.

Since 2012, **RED Technologies has developed extended know-how and a portfolio of patents** in the following domains:

- Spectrum Sharing,
- Cognitive Radio - Radio Environment Map (REM),
- Radio Propagation and Clutter Modeling,
- LTE Radio Network Engineering and Self Organizing Networks,
- Standards (ETSI, 3GPP, Wireless Innovation Forum),
- Geographical Information System (GIS),
- High Performance Computing,
- Database development, security, networking, cloud, and web.

For many years, RED Technologies has been working closely with Qualcomm, Ericsson and Nokia on research projects, demonstrations, pilots and regulatory and standardization activities involving spectrum sharing.

RED Technologies headquarters is based at 130, rue de Lourmel, Paris, France.

Figure 5: RED Technologies' premises, Paris, France

4.1.2. Founders

The company was founded by

- **Pierre-Jean Muller** (47), a telecommunications executive veteran with 25 years of international experience within the wireless industry including six years with Bell Labs in France, UK and Germany. Pierre-Jean is a frequent speaker at international technology conferences and has hosted several elected positions in ETSI and 3GPP. He is the author of 20+ patents in the telecommunication field.
- **Michael Abitbol** (46), a senior executive with extensive experience in business development and management in Asia, Europe and the US, having founded, managed and held executive positions in international companies both within and outside the telecommunications sector.

4.1.3. Board of directors

The company's board of directors comprises its founders Pierre-Jean Muller and Michael Abitbol, and:

- **Bruno Rambaud** brings 25+ years' experience in executive level positions at leading multinationals in the aeronautic, defense, space and security sectors (Airbus Defense & Space, Thales Communications and Security, Rockwell-Collins). Bruno has received the prestigious French Knight of the Legion of Honor award for his contribution to engineering and the French economy.
- **Joëlle Toledano** is Professor in Economics at CentraleSupélec and a Doctor of Mathematics and Economics. Joëlle has held executive-level positions in major French companies and was board member of the French regulator (ARCEP) from 2005 to 2011. In 2014, Joëlle was charged by the French Minister of State for the Digital Sector and Innovation to propose a set of recommendations on Dynamic Spectrum Management for Innovation and Growth (see Executive summary: http://www.economie.gouv.fr/files/files/PDF/french-spectrum-mission-executive-summary-2014-06-25.pdf). Joëlle has received the prestigious Medal of the National Order of Merit and is French Knight of the Legion of Honor.
- **Olivier Dubuisson** is General Manager and Partner at the French technology investment firm, Cap Décisif. Olivier is an engineer by training with experience in the defense (Thales) and telecoms sectors (Aqsacom).

4.1.4. Ownership structure

RED Technologies is a well-capitalized enterprise fully supported by its main shareholder Cap Décisif (see §6.6 Support letter from Cap Décisif).

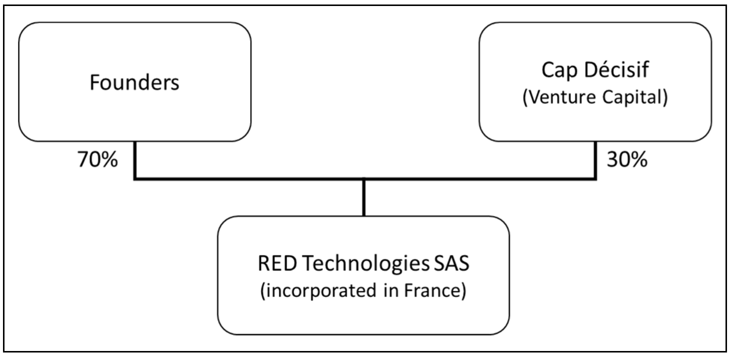


Figure 6: RED Technologies ownership structure

4.1.5. European R&D Team

The **unique expertise** and **diverse industry and academic connections** of this specialist team will be applied to the continuous innovation of the SAS solution. In addition, we expect to see fruitful idea exchange across our European and US team members, partners and customer base as we evolve our LSA solution in parallel with SAS.

Our R&D team is a **multidisciplinary team composed of PhD holders and engineers** coming from the telecoms and wireless industry. Team members have worked for leading companies such as Alcatel-Lucent, Nokia, NEC and Thales in all major R&D functions:

- Project manager,
- Standardization,
- System and Software architecture,
- Software development,
- Test and validation,
- IT.

Altogether, their expertise covers the latest wireless technologies and software development skills:

- LTE, LTE-U, LAA,
- Cloud-RAN (CRAN)
- Cognitive Radio (CR) and Software Defined Radio (SDR),
- Propagation modelling,
- Spectrum sharing (TVWS, LSA, SAS).

4.2. RED TECHNOLOGIES USA, LLC

4.2.1. Ownership structure

To operate its SASlive© product (see §4.3.2, §6.3.2) by a dedicated service center (see §5.1) in North America, **RED Technologies' is setting-up RED Technologies USA, LLC**.

RED Technologies USA, LLC will be a fully owned subsidiary, in Arlington, Virginia and will hire qualified personnel for operating the SAS locally. The proposed ownership structure is the following:

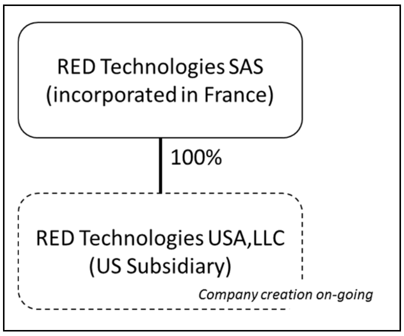


Figure 7: RED Technologies USA, LLC, ownership structure

RED Technologies USA, LLC will administrate the SAS operation for the US with the help of local and qualified staff.

Through the creation of its US subsidiary, RED Technologies will generate local jobs, foster US innovation and humbly contribute towards reducing the country's digital divide by enabling better access to Information and Communication Technologies (ICT) through the 3.5 GHz Citizens Broadband Radio Service band opportunity.

4.2.2. Organization

This US subsidiary will rely on three departments:

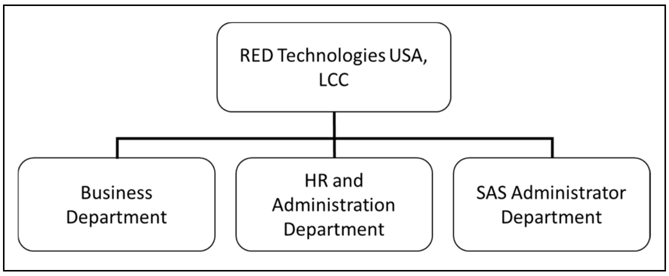

RED Technologies USA, LCC
Business Department
HR and Administration Department
SAS Administrator Department

Figure 8: RED Technologies USA, LCC organization

- A Business Department to identify new customers and market and sell the RED Technologies' SASlive© services in accordance with RED Technologies' business strategy (see §4.2.3).
- A HR and Administration Department to recruit and manage local staff and perform administrative tasks.
- A SAS Administrator Department to operate and maintain the SAS (see §5.1).

In addition to this physical office, **RED Technologies shall create an on-line identity through the development of a RED Technologies USA, LLC website**. The website shall be a key business development and recruitment tool as well as a primary support for marketing both the attributes of the 3.5 GHz CBRS band and RED Technologies' solutions.

4.2.3. Business strategy

RED Technologies firmly believes that shared spectrum will create new commercial opportunities.

Cellular (LTE) services have made available a considerable number of frequency bands but these are assigned on an exclusive basis and are operated by "happy few" carriers.

The 3.5 GHz CBRS band opens up disruptive new models such as neutral host and private networks.

Neutral host allows deployments using common spectrum and common deployment and provides neutral host services (like Wi-Fi). However, while it is deployable as a standalone / private network, neutral host can interwork with legacy 3GPP carrier networks. This creates a fresh win-win situation because carriers that did not intend to deploy in-building or rural outdoors, can gain access to a much broader footprint

Neutral Host addresses the issues that many venue owners and enterprise IT leaders experience with in-building wireless. These include poor cellular coverage for voice services, overutilization of the 5 GHz Wi-Fi band, and a need for higher quality wireless data services.

Neutral Host native capabilities allow a local service provider network to support subscribers of multiple nationwide carriers within buildings thanks to the opportunity made possible by the 3.5 GHz CBRS band to deploy cellular (LTE) services without the "barrier-to-entry" expense of fully licensed spectrum.

RED Technologies USA, LCC will focus its business development on those **local service providers** offering a dedicated SAS service, PAL "Lessor/Lessee" optimized spectrum coordination and a REM-based interference management system specialized for in-building CBSD deployment.

RED Technologies believes that once the 3.5 GHz CBRS band is deployed and commercially proven, the model will be exported and deployed globally and potentially extended to many other frequency bands in sub 1 GHz, sub 6 GHz and millimeter wave (mmWave) spectrum to feed much anticipated spectrum needs for 5G.

4.3. RED TECHNOLOGIES PRODUCTS

Today, RED Technologies develops two products in the field of dynamic spectrum sharing:

- LSAlive© for European market (see §4.3.1, §6.3.1),
- SASlive© for North American market (see §4.3.2, §6.3.2).

These two products have already been deployed with demonstrators and pilots in partnership with industry and regulators. The products have also been integrated within testbeds in the context of European Commission R&D projects.

This proposal for Spectrum Access System Administrator only concerns RED Technologies' SASlive© product.

4.3.1. LSAlive© product

The company deployed its LSAlive© product as part of the realization of two large **pilot projects** in Europe:

- **2.3 GHz LSA Pilot, Rome, Italy, 2015**
- **2.3 GHz LSA Pilot, Paris, France, 2016**

In addition to these pilot projects, RED Technologies is also involved in two **European Research Projects** on spectrum sharing.

The following projects are funded by the European Commission's Directorate General for Communications Networks, Content & Technology (DG CONNECT), under its 7th (FP7) and 8th (H2020) EU Framework Program for Research and Technological Development:

- **2.3 GHz FLEX LSA, 2016,**
- **3.5 GHz WISHFUL RADARLSA, 2017.**

4.3.1.1. 2.3 GHz LSA Pilot, Rome, Italy, 2015

RED Technologies provided the license-shared access (LSA) platform (see §6.3.3.1) for the first large scale 2.3 GHz LSA pilot implemented in Rome, Italy.

The pilot was launched in Rome in 2015 by the Italian Ministry for Economic Development and the Joint Research Centre of the European Commission to validate the technical conditions for spectrum sharing in the 2.3 GHz band. Using the CEPT approach to LSA, the pilot enabled the definition of a sharing framework for LSA between incumbents (PMSE, fixed links and government users) and mobile broadband providers. The LSA architecture employed in the Rome pilot was implemented in conformance with the ETSI draft standard.

The network deployment used in Rome focused on micro and small cells scenarios. The pilot was a testbed for investigating not only spectrum sharing from a regulatory perspective, but also research issues related to the emerging challenge of 5G communications. The pilot lasted 12 months. Other main participants were **Nokia, Qualcomm** and Fondazione Ugo Bordoni (FUB) – see IEEE DySPAN 2017 #1570321677 ('Sharing Under Licensed Shared Access in a Live LTE Network in the 2.3-2.4 GHz Band End-to-end Architecture and Compliance Results').

4.3.1.2. 2.3 GHz LSA Pilot, Paris, France, 2016

In Paris in 2016, RED Technologies together with **Ericsson and Qualcomm** demonstrated live the world's first LTE Advanced Carrier Aggregation integrated with LSA in the 2.3 GHz spectrum band (see §6.3.3.2).

The use of the 2.3 GHz band was authorized by the French Department of Defense. The pilot lasted six months - http://www.redtechnologies.fr/news/enabling-5g-red-technologies-ericsson-and-qualcomm-demonstrate-licensed-spectrum-sharing-solutions-mobile-world-congress.

World's first Licensed Shared Access with carrier aggregation pilot
Premier pilote mondial LSA avec agrégation de porteuses
ERICSSON
QUALCOMM
RED
Premier pilote mondial LSA avec agrégation de porteuses
World's first Licensed Shared Access with carrier aggregation pilot

In January 2016, the 2.3 GHz LSA pilot was **inaugurated by the French Minister of State for the Digital Sector and Innovation**, Axelle Lemaire, who reported to the Minister of the Economy and Finance.

4.3.1.3. European Commission project - 2.3 GHz FLEX LSA

The main objective of the FLEX LSA experiment (see §6.3.5.1) is to test, for the first time, the latest ETSI specifications of LSA in a multi-country / multi-regulatory framework set-up. This is being achieved using new software modules brought by new partners together with existing LTE base stations (eNB) deployed onto the FLEX testbeds (EURECOM in France and NITOS in Greece).

The outcome of this project contributed to the LSA standardization process in ETSI Reconfigurable Radio Systems (RRS) and 3GPP.

4.3.1.4. European Commission project - 3.5 GHz WISHFUL RADAR LSA

Traditionally the implementation of LSA follows a semi-static spectrum sharing model where exclusion zones for incumbents' protection are stable and can be activated or deactivated based on timing information (i.e. start/stop times).

The main objective of this experiment (see §6.3.5.2).is to test a functional implementation of the LSA framework enhanced by spectrum sensing, considering the scenario of military radars operating at 3.5 GHz band.

The experiment is using the WISHFUL unified programming interfaces and the IRIS testbed for end-to-end experimentation.

This experiment can be considered as the first-time demonstration of a possible reconciliation path between ECC LSA 2-Tier framework and FCC 3.5 GHz 3-Tier CBRS framework

4.3.2. **SASlive© product**

RED Technologies demonstrated live, for the first time, its SAS implementation integrated with pre-commercial TD-LTE CBSDs and CPEs in the 3.5GHz band (see §6.3.4, §6.4), at the European Telecommunications Standards Institute (ETSI) Radio Virtual Machine & Security for Multi-RAT Reconfigurable Systems workshop that took place **on March 10, 2016**.

At this meeting, ETSI hosted RED Technologies to demonstrate the effectiveness of its Spectrum Access System (SAS) solution in the 3.5 GHz band. A live demonstration took place in Rennes, France hosted by <B-Com> and attended by major global carriers and equipment manufacturers. This demonstration (for which RED Technologies obtained the necessary authorization to use the 3.5GHz spectrum from a French operator) represents another important step towards the wide-scale adoption of new spectrum sharing approaches.

The testbed included a multi-tier 3.5 GHz RAN operating in the 3550MHz – 3700MHz frequency band and managed by RED Technologies' latest Domain Proxy (DP) SAS servers. The shown use cases cover 2nd Priority Access Licenses (PALs) and 3rd General Authorized Access (GAA) tier spectrum evacuation upon primary user detection with automatic radio network reconfiguration. - http://www.redtechnologies.fr/news/red-technologies-demonstrates-live-sas-35ghz-etsis-radio-virtual-machine-security-multi-rat-reconfigurable-systems-workshop -

For completeness, several screenshots of the current SAS implementation are given to illustrate the SASlive© product maturity and RED Technologies' know-how (see §6.4)

4.4. TECHNICAL CAPABILITY

RED Technologies is technically competent to develop, test and receive certification for its SAS system, in compliance with Commission rules and Wireless Innovation Forum standards.

RED Technologies leveraged its SASlive© product development and testing from its field tested LSAlive© platform which was operated during multiple-month field trails in Rome, Italy in partnership with Nokia and Qualcomm, and in Paris, France in partnership with Ericsson and Qualcomm.

Since 2012 the company has developed **extended know-how** in the following domains:

- Spectrum Sharing,
- Cognitive Radio - Radio Environment Map (REM),
- Radio Propagation and Clutter Modelling,
- LTE Radio Network Engineering and Self Organizing Networks,
- Standards (ETSI, 3GPP, Wireless Innovation Forum),
- Geographical Information System (GIS),
- High Performance Computing,
- Database development, security, networking, cloud, and web.

RED Technologies received the prestigious Business France, Best Telecom Innovation Award at Mobile World Congress in 2015 (MWC) - https://www.linkedin.com/pulse/mwc15-red-technologies-receives-best-telecom-award-2015-abitbol?trk=pulse-det-nav_art.

4.5. FINANCIAL CAPABILITY

RED Technologies has the funds and access to capital to support customer pilots, commercial launches and to operate the proposed SAS service for a **five-year term** in compliance with Commission rules.

RED Technologies is a well-capitalized enterprise fully **supported by its main shareholder** Cap Décisif (see §6.6 Support letter from Cap Décisif).

RED Technologies adopts a clear business strategy for its US market (see §4.2.3).

In addition, **RED Technologies will charge its SAS customers** (PAL and GAA users) **fees for its spectrum management and others value added services** (see §5.1.1.4).

Consistent with the Commission's goal of encouraging the rapid development of 3.5 GHz devices and services, RED Technologies will charge PAL and GAA users, reasonable and competitive per-device registration fees. If requested, RED Technologies will work with the Commission to review its fees and modify such fees if they are found to be unreasonable by the Commission.

RED Technologies' cloud-based SAS deployment (see §5.2.5) operated by a local service center (see §5.1) will contribute to keeping operational expenditure low while providing SAS administration services that are fully compliant with the Commission's rules.

4.6. EXTERNAL PARTNERSHIPS

4.6.1. ESRI Inc

RED Technologies and ESRI Inc have established a partnership which allows RED Technologies to use ESRI products (ArcGIS for server, ArcGIS pro, ArcGIS online). This partnership guarantees RED Technologies access to ESRI latest product releases and dedicated support.

5. RED TECHNOLOGIES' SOLUTION

5.1. SAS ADMINISTRATION

5.1.1. SAS Administrator service center

5.1.1.1. Organization

RED Technologies, through its local subsidiary, will set up a **dedicated service center** located in Arlington, Virginia, to ensure the management and maintenance of its SAS operation. This entity is called **SAS Administrator.** It will provide a 24/7 service to customers, and will be based on a dedicated and qualified team using the SASlive© product realized by RED Technologies.

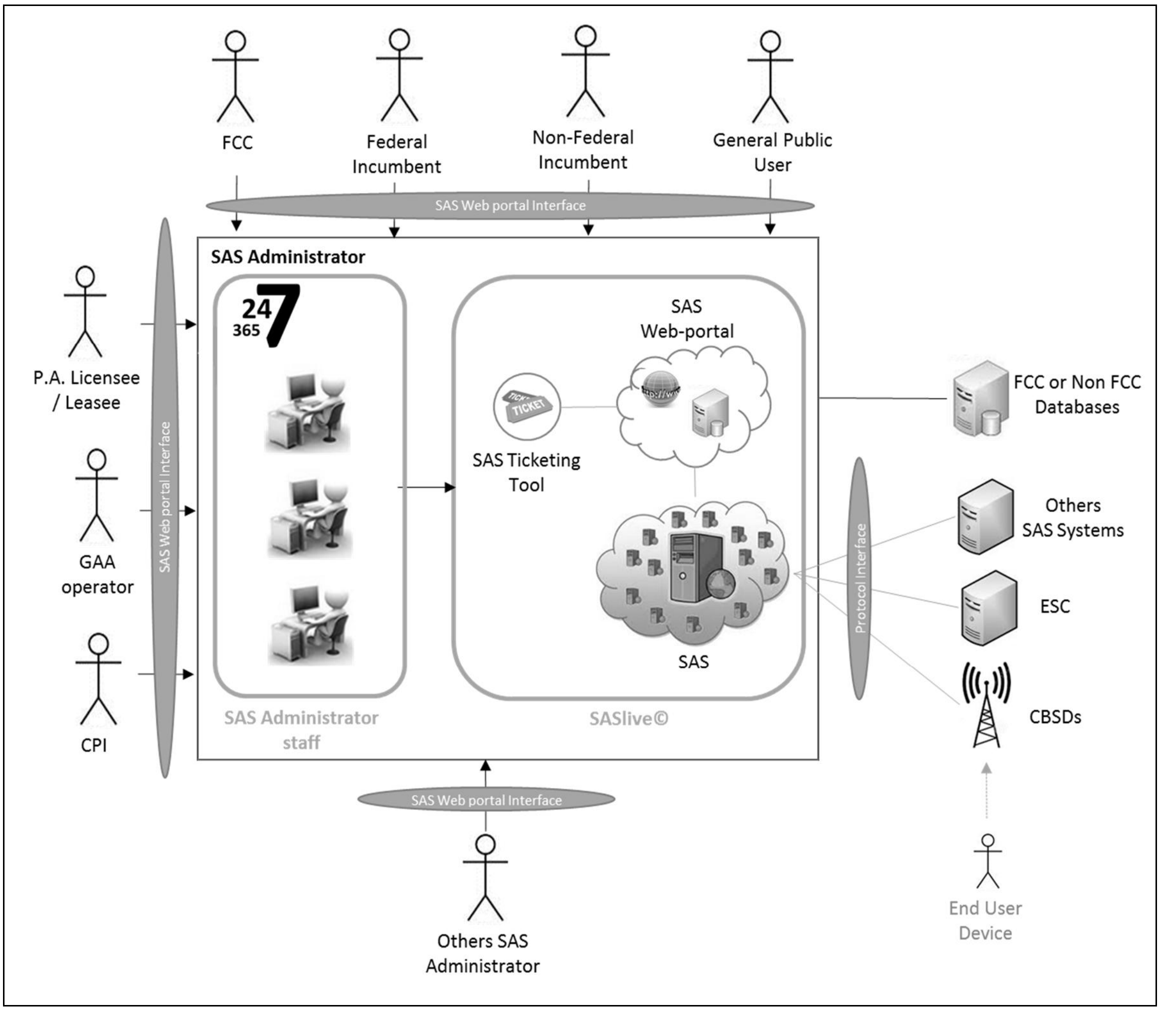


Figure 9 SAS Administrator and outside actors

As shown in the above diagram, RED Technologies will deploy a web portal to deal with requests coming from the different actors. These requests are registered into the SAS ticketing tool (see §5.2.1.3) before being treated.

RED Technologies will also put in place any means necessary and required (IT, hotline, process, legal, resources) to answer to exceptional request by the president or any governmental representative (see [Ref. 04] - 96.63(l))

5.1.1.2. Quality of Service

To measure the quality of the service provided by the SAS Administrator, RED Technologies, for its own use, will implement and monitor some specific indicators (SLA indicators).

If RED Technologies observes that the level of these indicators does not meet the required level and that the quality of service is decreasing, RED Technologies will be able to quickly take the action necessary to solve the problem. A causal analysis will also be performed to understand the origin of the problem and solve it.

5.1.1.3. Local Staff

To ensure the operational management and maintenance of the SAS Administrator, RED Technologies has identified the following required competencies:

- Radio network engineering,
- IT management (cloud, security, networking, software update),
- Database management.

RED Technologies will recruit a dedicated team with the above competencies when staffing its subsidiary in the USA.

Moreover, to ensure the competencies of the team on RED Technologies' SASlive© product and the others management tools, training and coaching sessions will be organized by the product development team in France.

5.1.1.4. Services

The SAS administrator provides a set of services sorted in three main categories:

- User Services (see §5.1.2):
    - These services are defined as mandatory by the FCC and allow users to interact directly with the SAS Administrator.
- Added Value User Services:
    - These services are complementary services that RED Technologies offers to its customers to help them to deploy their infrastructures and analyze the performance of their network through the implementation of strategic KPIs.

      These services are not described in this document but cover:

        - *PPA radio planning tool and ROI,*
        - *Spectrum and operation KPIs (Analytics tool),*
        - *Radio optimization support services.*
- Administration Services (see §5.1.3):
    - These services are reserved for RED Technologies staff for the operational maintenance and the administration of the SAS. They are not accessible to non-RED Technologies staff.

The following sections describe, in detail, these services.

5.1.2. **SAS Administrator - User Services**

5.1.2.1. Organization's Subscription Management

The subscription service allows an organization (FCC, Incumbent, Priority Access Licensee, and Certified Professional Installer (CPI)) to subscribe privileged access from the SAS administrator. Thanks to this subscription, the organization and its members, after authentication, can access information to which the general public does not have access.

The person requesting a subscription for his organization will be assigned a login and a password as well as the rights of "Organization's Administrator" on behalf of their organization. These special rights allow him/her to gain access to certain functions such as member registration on the SAS portal of his/her organization (see §5.1.2.2).

During the subscription, the access profile(s) for the members of the entity are defined. These profiles establish the services and the data that members of the organization can access, in accordance with FCC requirements.

This subscription phase does not concern the general public, which has the minimum right of access to services and data.

5.1.2.2. Organization's Users Account Management

Once the entity has subscribed to the offer of service from the SAS Administrator, the entity will have to register its members for them to access these services.

When registering, the SAS Administrator creates a personal account (with login and password) for each user and assign to them their user rights according to the defined access profile.

RED Technologies has identified the following services:

- Create a new user account,
- Delete a user account,
- Modify a user account,
- Change user password,
- Request new user password after being forgotten.

The workflow below illustrates in detail the « *Create a new user account* » service showing the different actors and the principle actions. The other services are not described, because they are very similar.

The actor, «organization's subscriber», represents FCC, P.A. Licensee, Federal government entity, Authorized user of the CBSD or FSS.

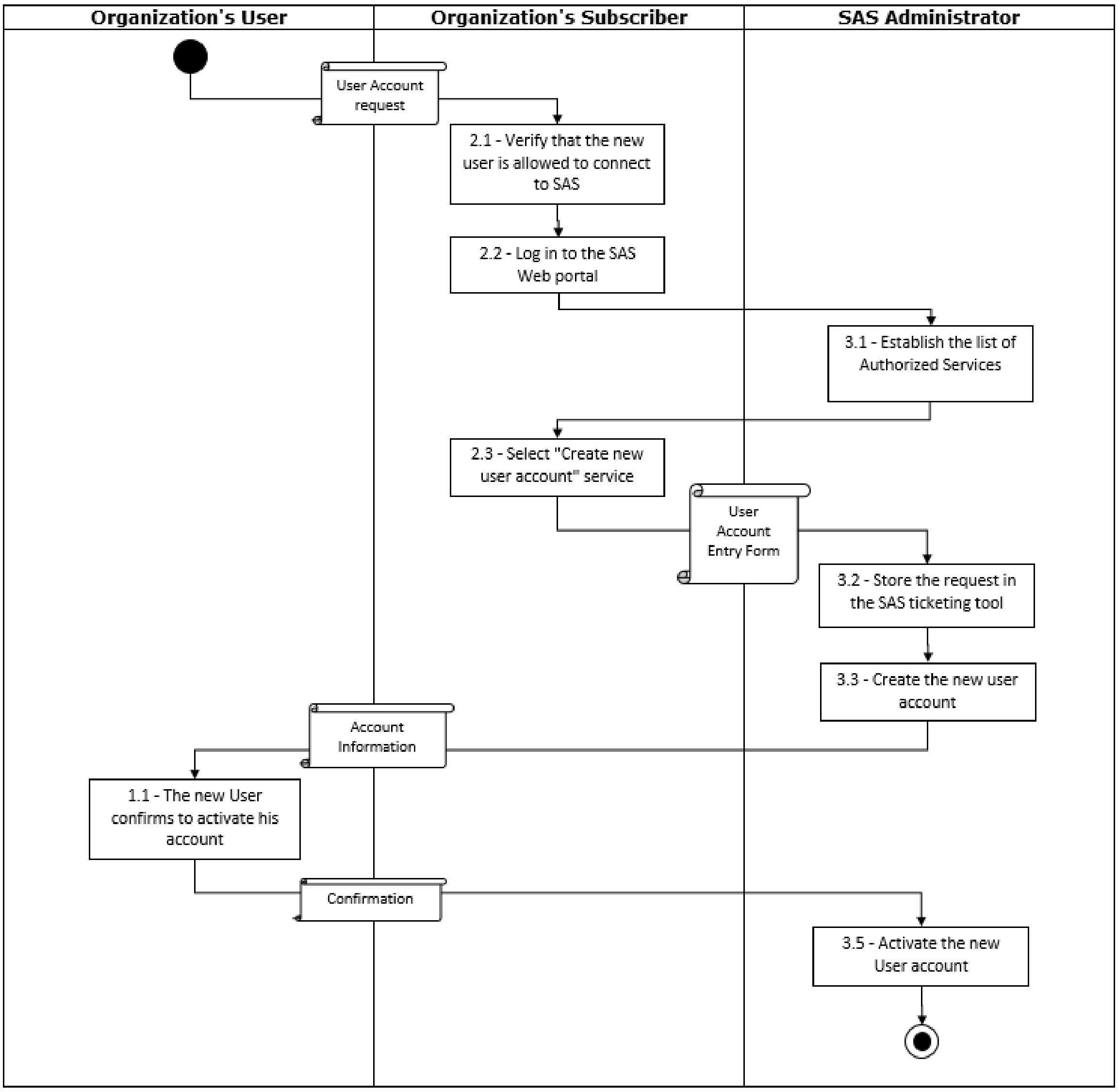

Organization's User
Organization's Subscriber
SAS Administrator
User Account request
2.1 - Verify that the new user is allowed to connect to SAS
2.2 - Log in to the SAS Web portal
3.1 - Establish the list of Authorized Services
2.3 - Select "Create new user account" service
User Account Entry Form
3.2 - Store the request in the SAS ticketing tool
3.3 - Create the new user account
Account Information
1.1 - The new User confirms to activate his account
Confirmation
3.5 - Activate the new User account

Figure 10: « Create a new user account » workflow

Step	Description
2.1	On reception of the request from an organization’s user, the organization’s subscriber verifies that this user is allowed to access to the SAS and defines its scope of access.
2.2	The organization’s subscriber logins to the SAS web portal with its login and password.
3.1	Once the organization’s subscriber is authenticated, the SAS Administrator establishes the list of services and data that are authorized for this organization.
2.3	From this list, the organization’s subscriber selects the service “Create new user account”, fills the entry form then submits its request.
3.2	The “Create new user account” request is logged in the SAS ticketing tool. Then, the SAS administrator analyzes the entry form and verifies that the information is correct. If not, the SAS administrator notifies the organization’s subscriber that the request is not correct and the missing information shall be added.
3.3	Once the request is accepted, the SAS administrator creates an account for the new user: • registers user information • creates a new login, • generates a new password then notifies the organization’s user by mail that his account had been created.
1.1	On reception of this notification, the organization’s user shall confirm his account before using it.
3.5	Once a confirmation is received, the SAS Administrator activates the new user’s account

Table 2: « Create a new user account » workflow description

5.1.2.3. Display and Export User Data Management

The SAS administrator handles a large amount of data which is stored in its databases. Some of this data is accessible by the general public, while other data is restricted and will be only accessible by authorized users (FCC, P.A. Licensee, Federal government entity, Authorized user of the CBSD or FSS).

To deal with these two data access cases, RED Technologies has identified two services defined in the table below.

In this table, the column "FCC Rules" refers the rule of the documents [Ref. 04] or [Ref. 05] covered by these services.

Actor	Service	FCC Rules
General public	Display and Export Public User Data	96.55 - a3 96.63 - j
Authorized User	Display and Export Authorized User Data	96.59 - a1 96.59 - a2

These two services are illustrated in the following workflows:

Workflow 1 - Display and Export Public User Data:

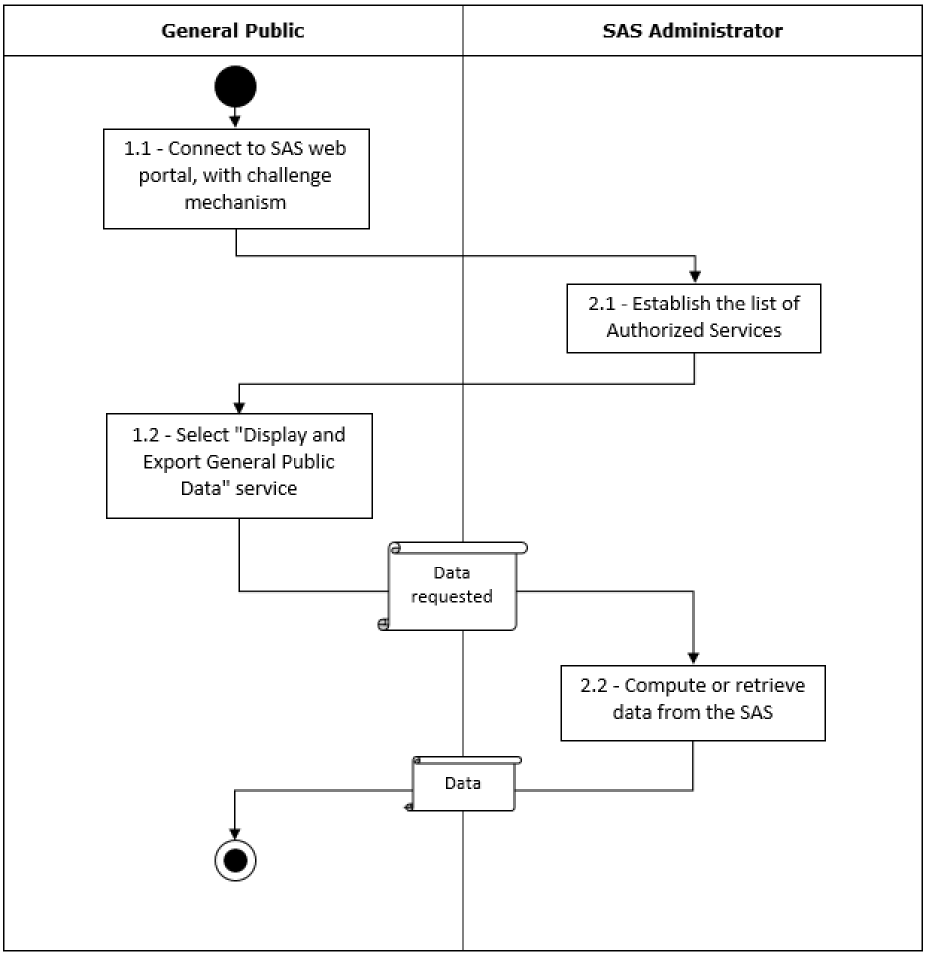

General Public
SAS Administrator
1.1 - Connect to SAS web portal, with challenge mechanism
2.1 - Establish the list of Authorized Services
1.2 - Select "Display and Export General Public Data" service
Data requested
2.2 - Compute or retrieve data from the SAS
Data

Figure 11: « Display and Export Public Data » workflow

Step	Description
1.1	The general public user connects to the SAS web portal without any login and password. Nevertheless, to differentiate robots from human clients a mechanism is implemented, based on challenge request. The SAS Web-portal sends a specific request to the user and waits for a specific response. If the answer is not the expected answer, this user is not considered as a human but a robot. In this case, the workflow is aborted.
2.1	Once the user is connected, the SAS Administrator establishes the list of services and data which are authorized for this general public user and sends this list to the user.
1.2	On reception of this list, the user selects a set of services and/or data and returns this information to the SAS Administrator.
2.2	When the SAS Administrator receives this information, it can: • Simply retrieve the requested data from the database, • Execute the services to compute and generate the requested data. Once available, the data is communicated to the user in the format requested (e.g. diagrams, table, map, list). Only non-restricted data is provided to the general public; for instance, the identities of the licensees will be obfuscated. Typically, information accessible to the general public is part of CBSD information.

Table 3: « Display and Export Public Data » workflow description

Workflow 2 - Display and Export Authorized User Data:

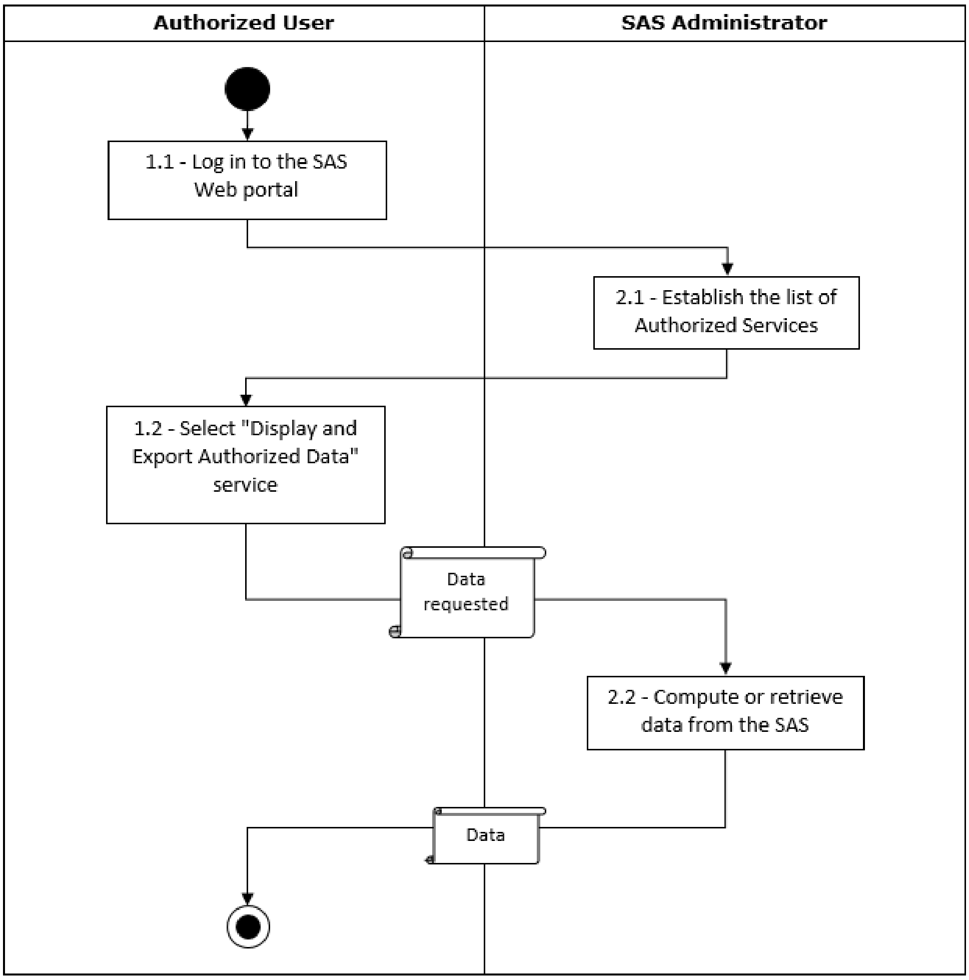

Authorized User
SAS Administrator
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Display and Export Authorized Data" service
Data requested
2.2 - Compute or retrieve data from the SAS
Data

Figure 12: « Display and Export Authorized Data » workflow

Step	Description
1.1	The authorized user logs in to the SAS web portal with his/her login and password.
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data which is authorized for this user and sends him/her this list.
1.2	On reception of this list, the user selects a set of services and/or data and returns this information to the SAS Administrator.
2.2	When the SAS Administrator receives this information, it can: • simply retrieve the requested materials from the database • execute the services to compute and generate the requested data: Once available, the data is communicated to the user in the format requested (e.g. diagrams, table, map, list)

Table 4: « Display and Export Authorized Data » workflow description

5.1.2.4. Data Control Management

The SAS handles a large amount of data stored in its database. This data come either from:

- External databases (see §3.2.3 and 3.2.4),
- Other administrators' SASs,
- CBSDs,
- CPIs,
- Licensees,
- or generated by the SAS for its own needs.

If the FCC or a party brings a claim of SAS data inaccuracy, verification, correction or removal of that data can be requested. To deal with this, the SAS Administrator proposes two services:

Actor	Service	FCC Rules
Authorized User	Verify Data	96.63 – f 96.63 – k
Authorized User	Correct/Suppress Data	96.63 - f

The workflow below illustrates the case "Verify Data". The second case being very similar is not described. This second case will be used to modify or remove some information from the SAS following the decision from the Authorized User.

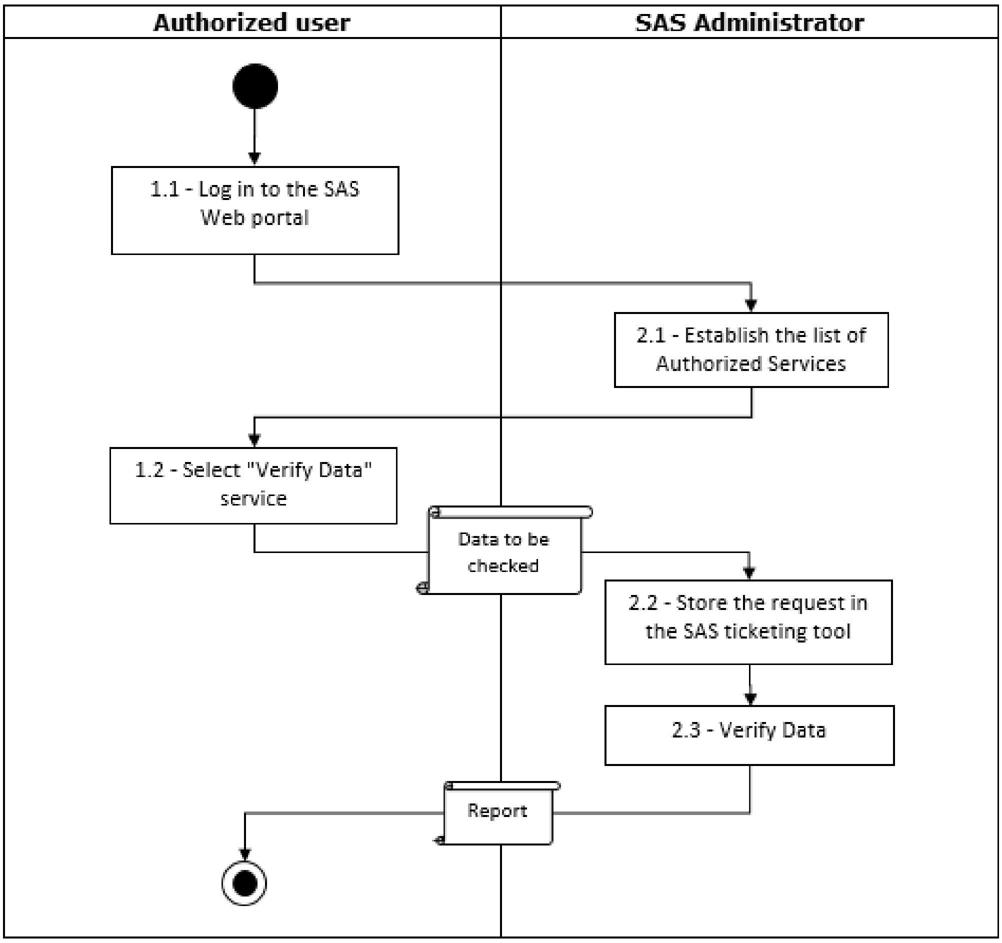

Authorized user
SAS Administrator
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Verify Data" service
Data to be checked
2.2 - Store the request in the SAS ticketing tool
2.3 - Verify Data
Report

Figure 13: « Verify Data in SAS » workflow

Step	Description
1.1	The Authorized User logs in to the SAS web portal with his/her login and password.
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data that is authorized for this user and sends him/her this list.
1.2	On reception of the list, the user selects the service "Verify Data" and provides the data to be checked.
2.2	The "Verify Data" request is logged in the SAS ticketing tool before being dealt with.
2.3	The SAS Administrator compares the data provided with that stored in the SAS. This verification is realized manually or with a script run by the SAS Administrator depending on the nature of the data provided. If some data is different, the SAS Administrator makes a root cause analysis to understand the reason. Then, if needed, the SAS Administrator updates the data in the SAS. Once the analysis is completed, the Administrator returns a report to the user.

Table 5: « Verify Data in SAS » workflow description

5.1.2.5. Fee Information Management

SAS Administrators can collect reasonable fees from Priority Access Licensees and General Authorized Access users for the use of the SAS and added value services.

The calculation methods and the amount of the fees are **strictly confidential**. However, the FCC may request access to the fee information to verify that the price charged is not excessive and the FCC may ask for a readjustment of the fees if deemed necessary.

The SAS Administrator provides two services:

Actor	Service	FCC Rules
FCC	Get Fees Information	96.65 - a
FCC	Request to change Fees	96.65 - b

The workflow below illustrates the case "Get Fees Information". The second case being very similar is not described.

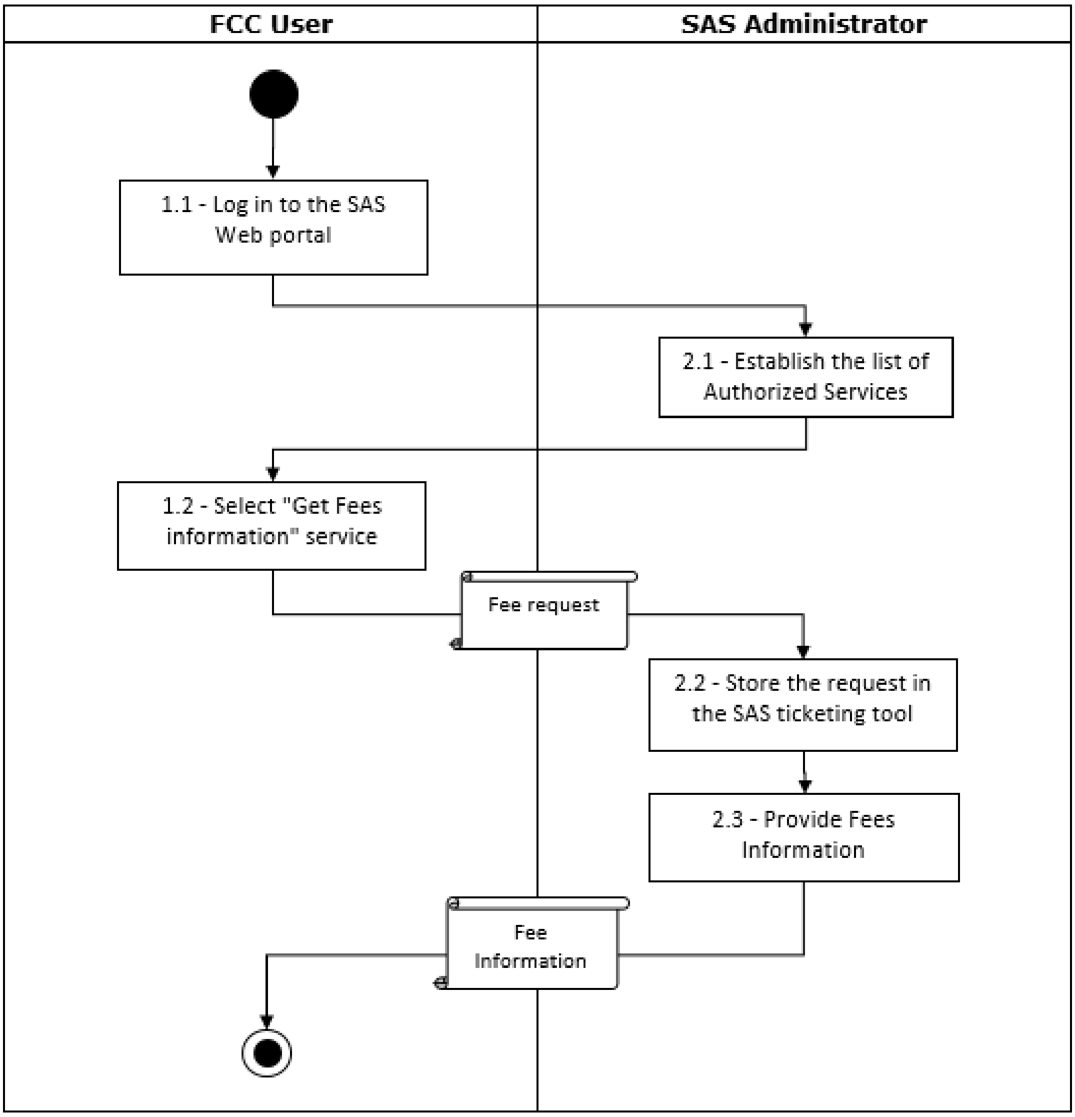

FCC User
SAS Administrator
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Get Fees information" service
Fee request
2.2 - Store the request in the SAS ticketing tool
2.3 - Provide Fees Information
Fee Information

Figure 14: « Get Fees Information » workflow

Step	Description
1.1	The FCC’s user logs in to the SAS web portal with his/her login and password.
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data that is authorized for this user and sends him/her this list.
1.2	On reception of the list, the user selects the service "Get Fees Information" and describes which kind of information he would like to receive.
2.2	In SAS Administrator, the "Get Fees Information" request is logged in the SAS ticketing tool.
2.3	The SAS Administrator analyzes the request and returns fee information the user.

Table 6: « Get Fees Information » workflow description

5.1.2.6. PAL Protection Area Management

The Priority Access Licensee shall notify the SAS Administrator their PAL Protection Areas, based on their network deployments.

The SAS validates the contiguous protection contour as a -96dbm /10MHz contour around deployed CBSDs using information collected through the CBSD registration.

The following service explains this behavior.

Actor	Service	FCC Rules
P.A. Licensee / Lessee	Validate and apply a PAL Protection Area	96.25-c
P.A. Licensee / Lessee	Modify a PAL Protection Area	96.25-c
P.A. Licensee / Lessee	Suppress a PAL Protection Area	96.25-c

The workflow below illustrates the case "Validate and apply a PAL Protection Area ". The other cases being very similar are not described.

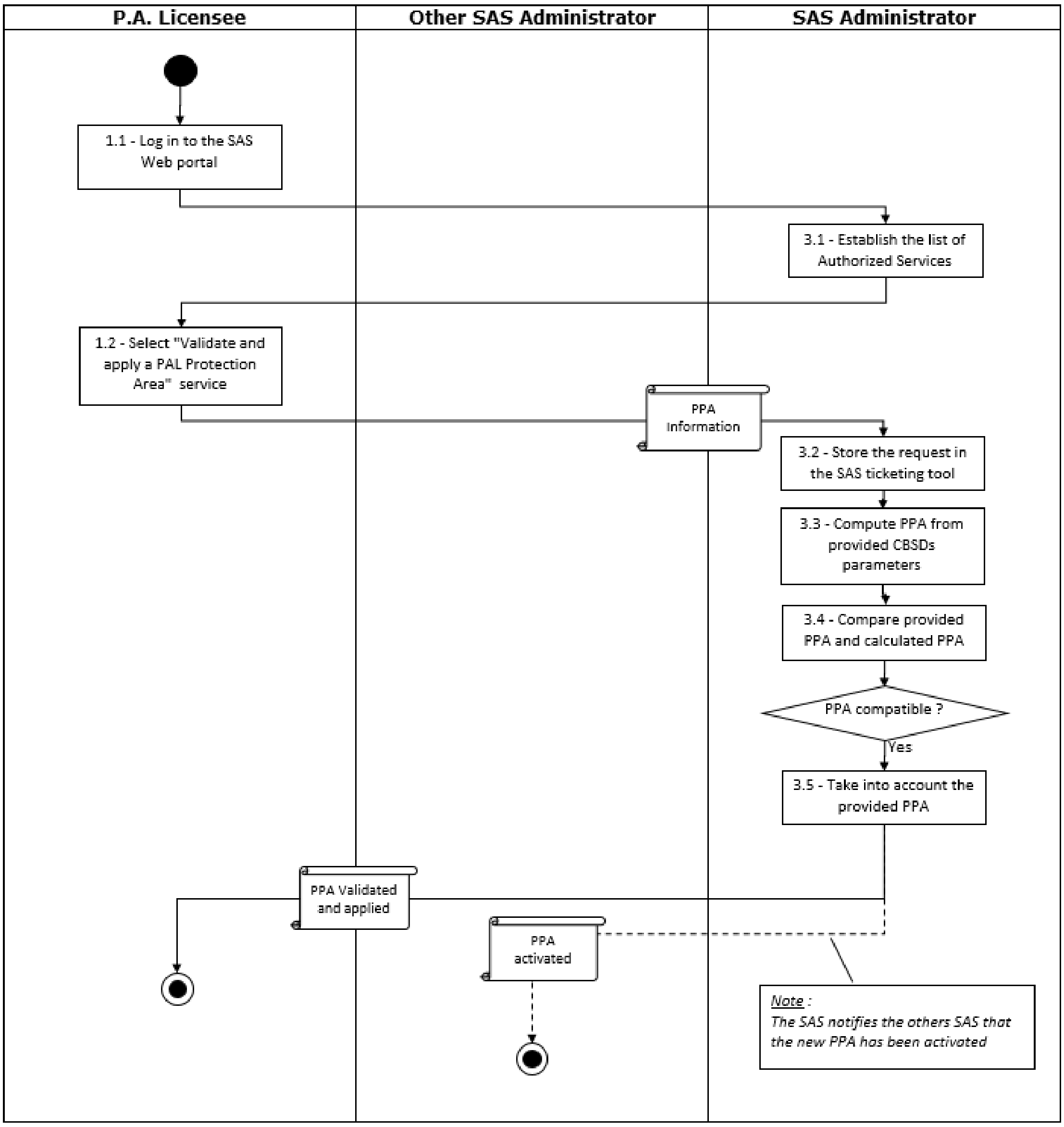

P.A. Licensee
Other SAS Administrator
SAS Administrator
1.1 - Log in to the SAS Web portal
3.1 - Establish the list of Authorized Services
1.2 - Select "Validate and apply a PAL Protection Area" service
PPA Information
3.2 - Store the request in the SAS ticketing tool
3.3 - Compute PPA from provided CBSDs parameters
3.4 - Compare provided PPA and calculated PPA
PPA compatible ?
Yes
3.5 - Take into account the provided PPA
PPA Validated and applied
PPA activated
Note :
The SAS notifies the others SAS that the new PPA has been activated

Figure 15: « Validate and apply a PAL Protection Area » workflow

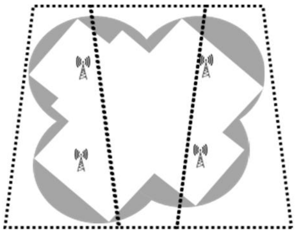
Step	Description
1.1	The P.A. Licensee user logs in to the SAS web portal with his/her login and password.
3.1	Once the user authenticated, the SAS Administrator establishes the list of services and data that are authorized for this user and sends him/her this list.
1.2	On reception of this list, the user selects the service "Submit and Validate a PAL Protection Area" and provides requested information (PPA contour and CBSD parameters)
3.2	The "Validate a PAL Protection Area" request is logged in the SAS ticketing tool before being dealt with.
3.3	The SAS Administrator, computes, from CBSD parameters, the effective PPA using standardized radio propagation models and algorithms. The calculated PPA (see §5.2.1.4.3.3) is determined by the SAS as a -96dBm/10MHz contour around each CBSD. Example PPA deployment on three census tracts: • provided PPA: white contour • calculated PPA: blue contour • census tracts: dot line contour 
3.4	The SAS Administrator compares the two PPA. If the provided PPA is not included within the calculated PPA, the request is aborted and a failure notification is returned to the P.A. Licensee.
3.5	When the provided PPA is included within the computed PPA, the PPA is validated, and the SAS Administrator: • registers the PPA into the SAS • confirms to the P.A. Licensee that the PPA is validated • broadcasts the PPA to other SAS Administrators when the PPA becomes active

Table 7: « Validate a PAL Protection Area » workflow description

5.1.2.7. Tier1 - Tier 2 protection

When an authorized user identifies an interference issue in its protection zone and/or site, he/she can send a request to the SAS Administrator to investigate the situation.

The authorized user can be:

- Federal Government entities,
- Operators of incumbent fixed-satellite earth stations,
- Operators of incumbent wireless broadband service stations operating in the 3650-3700 MHz band,
- Operators of networks protected by Priority Access licenses,
- Operators of network equipment licensed by GAA rules,
- Other SAS Administrators,
- ESC Operator.

The SAS administrator offers the following service:

Actor	Service	FCC Rules
Authorized User	Analyze an Interference Incident Report	96.53 - o

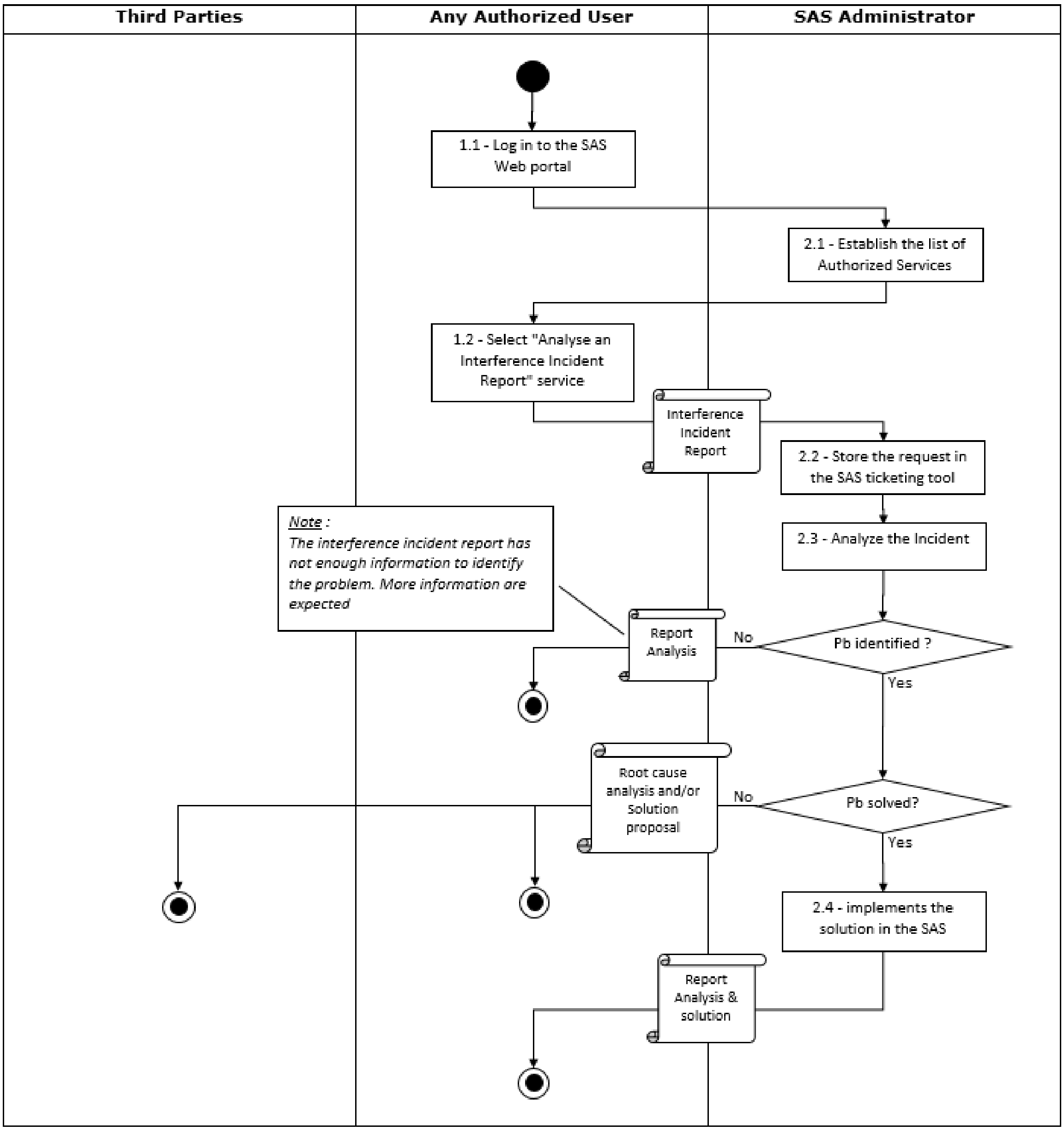

Third Parties
Any Authorized User
SAS Administrator
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Analyse an Interference Incident Report" service
Interference Incident Report
2.2 - Store the request in the SAS ticketing tool
2.3 - Analyze the Incident
Note : The interference incident report has not enough information to identify the problem. More information are expected
Report Analysis
No
Pb identified ?
Yes
Root cause analysis and/or Solution proposal
No
Pb solved?
Yes
2.4 - implements the solution in the SAS
Report Analysis & solution

Figure 16: « Analyze an Interference Incident Report » workflow

Step	Description
1.1	The Authorized User logs in to the SAS web portal with his/her login and password.
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data that are authorized for this user and sends him/her this list.
1.2	On reception of the list, the user selects the service "Analyze an Interference Incident Report", provides his report and details his request.
2.2	The "Analyze an Interference Incident Report" request is logged in the "SAS ticketing tool"
2.3	The SAS Administrator, analyzes the incident report: • Case 1: Incident can be resolved by the SAS Administrator The SAS Administrator implements the solution in its SAS • Case 2: Incident cannot be resolved by the SAS Administrator, but the causes of the incident have been identified The SAS Administrator forwards the Interference Incident Report to the Authorized User and the third parties for resolution with its own analysis. • Case 3: Other cases

	Interference Incident Report information is not enough to solve the issues, more information is requested to the sender. In the three cases, the user is informed back by status report.

Table 8: « Analyze an Interference Incident Report » workflow description

The Third Parties can be:

- The others SAS Administrators which are in a geographical area close to or within the zone concerned by the interference report and whose CBSDs may have an impact on this zone.
- Licensees which operate CBSDs.

5.1.2.8. Configure CBSD

All radio propagation computations performed by the SAS are based on the location of the CBSDs. The location reliability is therefore important and, for certain deployment types, are realized by certified professional installers, called CPI.

Services below allow a CPI to provide the location and other CBSD parameters directly to the SAS Administrator (the other case "Modify CBSD configuration" being very similar is not described).

Actor	Service	FCC Rules
CPI	Configure CBSD	96.39-a2 96.39-a3
CPI	Modify CBSD configuration	96.39-a2 96.39-a3

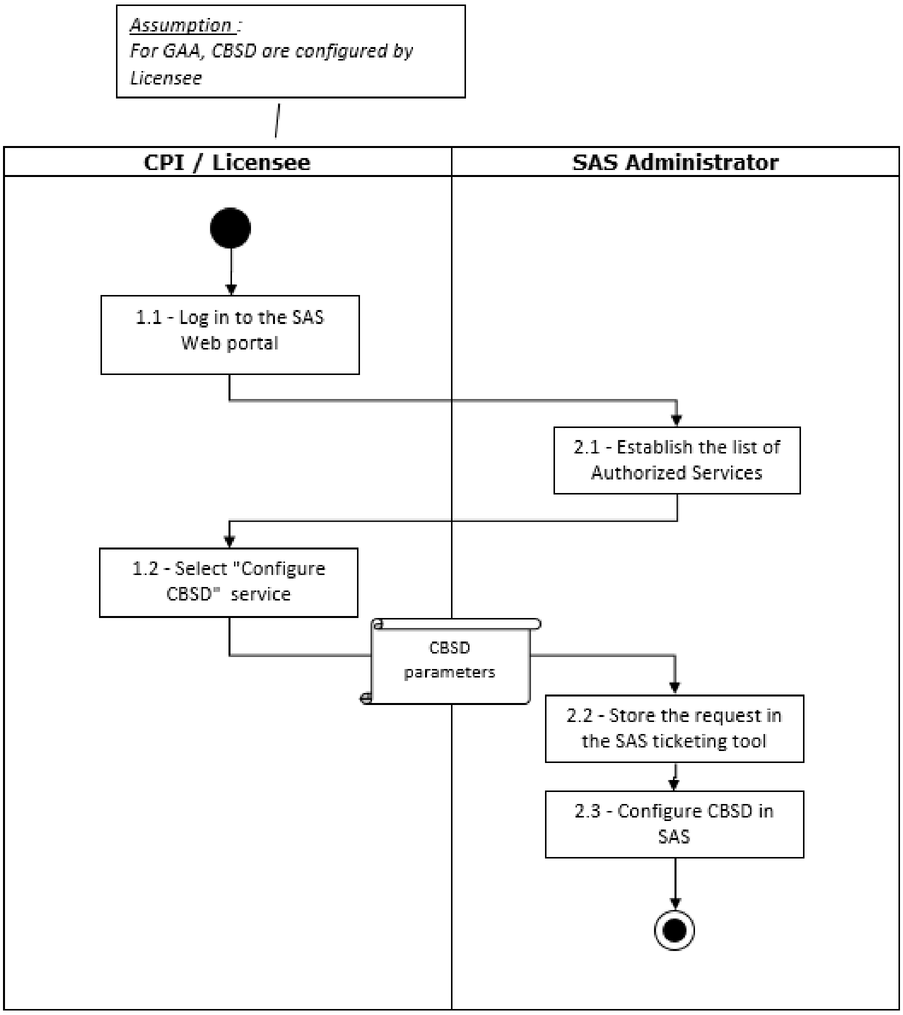

Assumption :
For GAA, CBSD are configured by Licensee
CPI / Licensee
SAS Administrator
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Configure CBSD" service
CBSD parameters
2.2 - Store the request in the SAS ticketing tool
2.3 - Configure CBSD in SAS

Figure 17: « Register CBSD parameters » workflow

Step	Description
1.1	The CPI or Licensee logs in to the SAS web portal with his/her login and password.
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data that are authorized for this user and sends him/her this list.
1.2	On reception of the list, the user selects the service "Configure CBSD" and provides the relevant parameters of CBSD.
2.2	The "Configure CBSD" request is logged in the "SAS ticketing tool"
2.3	When the SAS Administrator receives this list, it initializes the CBSD parameters in the SAS for requested CBSD.

Table 9: « Register CBSD parameters » workflow description

5.1.2.9. Leasing arrangement

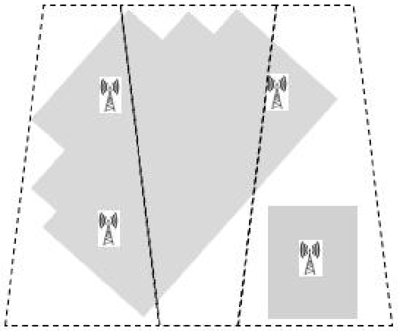
A Licensee who has purchased licenses for one or more census tracts may only decide to cover a part of those census tracts and set its PPAs accordingly. The licensee may decide to lease the area that it does not use within the PALs.

e.g.:

A Licensee bought PALs for its three census tracks defined by dot line in the diagram on the right.

The grey area defines the PPA of the Licensee. This PPA does not cover all the census tract.

In this case, the Licensee can decide to lease an unused part of its PAL area (yellow part) to another operator.



RED Technologies has identified four services:

- Register leasing arrangement,
- Extend leasing arrangement,
- Notify expiration of leasing arrangement,
- Deregister leasing arrangement.

The workflow below describes in detail the « Register leasing arrangement » service. The three other services are not described, because they are very similar.

Actor	Service	FCC Rules
Licensee	Register leasing arrangement	96.32 96.66 - a1 96.66 - a3 96.66 - a4 96.66 - a5
Licensee	Extend leasing arrangement	96.66 - a2
Licensee	Notify expiration of leasing arrangement	96.66 - a2
Licensee	Deregister leasing arrangement	96.66 - a2

Precondition: lessor and lessee shall agree on leasing.

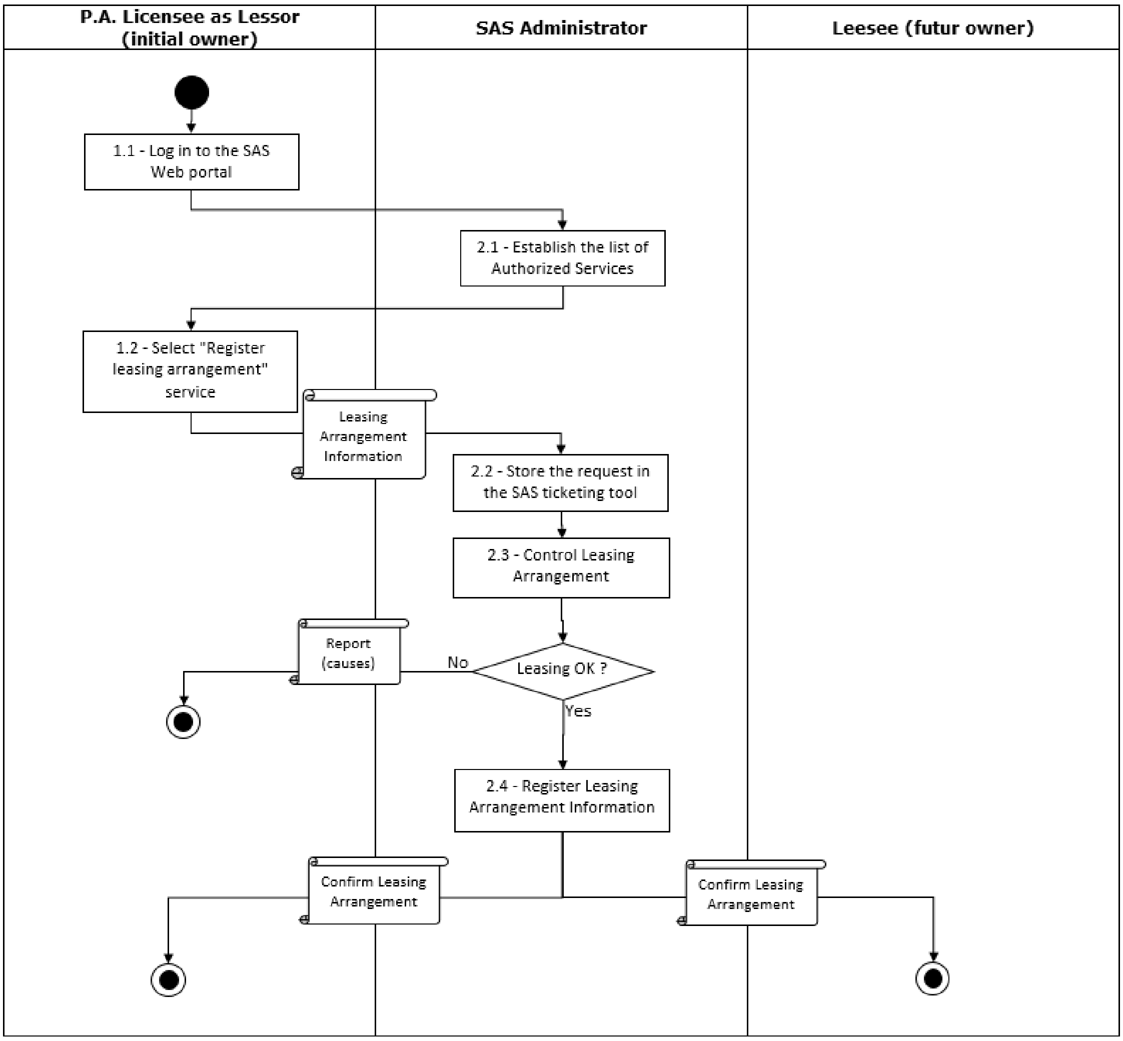

P.A. Licensee as Lessor (initial owner)
SAS Administrator
Leesee (futur owner)
1.1 - Log in to the SAS Web portal
2.1 - Establish the list of Authorized Services
1.2 - Select "Register leasing arrangement" service
Leasing Arrangement Information
2.2 - Store the request in the SAS ticketing tool
2.3 - Control Leasing Arrangement
Report (causes)
No
Leasing OK ?
Yes
2.4 - Register Leasing Arrangement Information
Confirm Leasing Arrangement
Confirm Leasing Arrangement

Figure 18: « Register leasing arrangement » workflow

Step	Description
1.1	The lessor user logs ins to the SAS web portal with his/her login and password
2.1	Once the user is authenticated, the SAS Administrator establishes the list of services and data that are authorized for this user and sends him/her this list.
1.2	On reception of the list, the user selects the service "Register leasing arrangement" and provides and completes the entry form with the requested information.
2.2	The "Register leasing arrangement" request is logged in the "SAS ticketing tool"
2.3	On reception of the Leasing registration request, the SAS Administrator shall realize the following verifications: • verify that the lessee is on the certification list of the FCC, • verify that the lease will not result in the lessee holding more than the 40 megahertz of priority access spectrum in a given license area • verify that the area to be leased is within the priority access licensee’s service area and outside of the priority access licensee’s PAL protection area If the verification fails, the leasing request is aborted and the licensee is notified.
2.4	If all leasing information is correct, the SAS Administrator registers this information in the SAS and notifies the lessor and the lessee users that the leasing registration is complete and successful.

Table 10: « Register leasing arrangement » workflow description

5.1.2.10. End of Administration Service Management

If RED Technologies does not continue as an SAS Administrator at the end of its term, RED Technologies will transfer relevant SAS information (including IP addresses, URLs used to access the system, and a list of registered CBSDs) to another SAS Administrator. This transfer will be secured and this service could be charged at a reasonable price.

Actor	Service	FCC Rules
Another SAS Admin	Transfer SAS Data to another SAS Administrator	96.63 - g

The workflow of this services is described below.

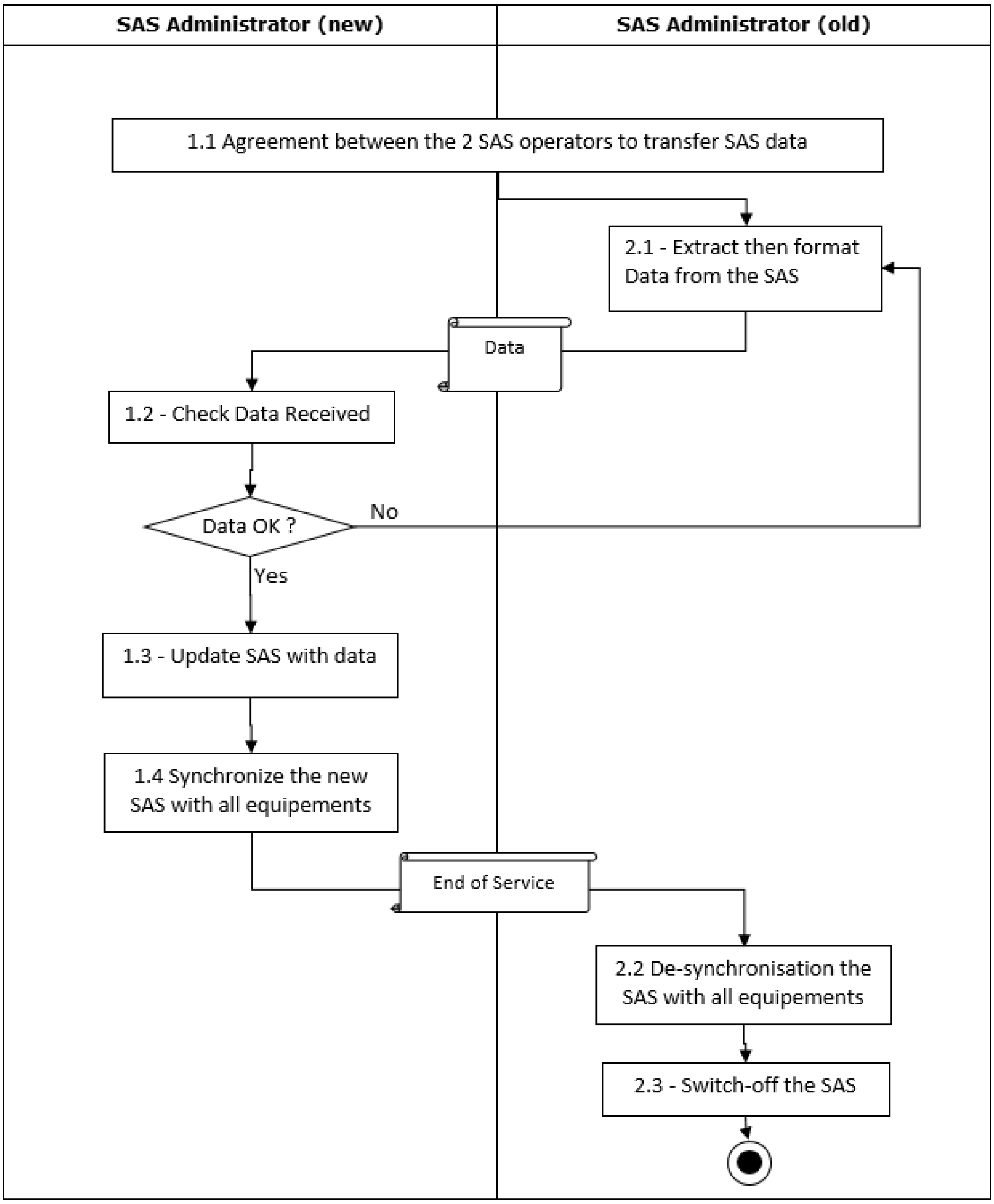

SAS Administrator (new)
SAS Administrator (old)
1.1 Agreement between the 2 SAS operators to transfer SAS data
2.1 - Extract then format Data from the SAS
Data
1.2 - Check Data Received
Data OK ?
No
Yes
1.3 - Update SAS with data
1.4 Synchronize the new SAS with all equipements
End of Service
2.2 De-synchronisation the SAS with all equipements
2.3 - Switch-off the SAS

Figure 19: « Transfer SAS Data to another SAS Administrator» workflow

Step	Description
1.1	Once the SAS Administrator activity transfer agreement is finalized, the transfer of data can be realized.
2.1	The old SAS Administrator extracts from its SAS all useful and necessary data for the new SAS administrator. This data is formatted in a format agreed between the two SAS Administrators and then stored on a server provided by the new SAS Administrator (IP addresses and URLs used to access the new SAS Administrator system).
1.2	The new SAS Administrator verifies that the all data have been correctly received, otherwise a new request is addressed to the SAS.
1.3	The new SAS Administrator considers the data received from the old SAS Administrator and updates its SAS.
1.4	The new SAS Administrator informs the equipment (ESCs, other SASs, CBSDs) that from now it is operational and synchronizes with them, then notifies the old SAS Administrator that it has taken control of the operations.
2.2	The old SAS Administrator informs the equipment that it will suspend its activity as SAS Administrator.
2.3	The old SAS Administrator switches off its SAS.

Table 11: « Transfer SAS Data to another SAS Administrator» workflow description

5.1.2.11. Other services

If a user wants to address a specific request that is outside of the above user services, the user can register its request using this generic service.

This service can be requested in the following case:

- To notify the SAS Administrator that there is a mutual agreement between a set of FSS earth stations and an authorized user of CBSDs to allow CBSDs to operate within areas that may cause interference to the given FSS earth station (see [Ref. 04] or [Ref. 05] FCC rule **96.17 – e**),
- For FSS earth station licensees in the 3600-3700 and 3700-4200 MHz bands, to request additional protection from SAS Administrators to prevent harmful interference into their systems (see [Ref. 04] or [Ref. 05] FCC rule **96.17 – f**),
- To deal with a demand coming from the President of the United States, or another designated federal government entity, issued pursuant to 47 U.S.C. 606 (see [Ref. 04] or [Ref. 05] FCC rule **96.63 – l**),
- To respond to requests from FCC for information stored or retained by the SAS (see [Ref. 04] or [Ref. 05] FCC rule **96.63 – k**)
- To consider enforcement instructions coming from the FCC (see [Ref. 04] or [Ref. 05] FCC rule **96.63 – m**),
- Any other cases.

5.1.2.12. CPI e-learning

RED Technologies will also offer a training service for CPIs to guide them in the use of the SAS web portal according requirements of [Ref. 14]. This service based on e-learning modules will be accessible from the web portal and their access account.

Upon completion of the training, RED Technologies will validate the knowledge gained by the CPI with an online test and will issue a certificate if successful. It is only once this certificate has been obtained that the CPI will be authorized to access the relevant functionalities of the web-portal.

5.1.3. SAS Administrator - Administration Services

Administration services are performed by the staff of the SAS Administrator. They mainly concern SAS maintenance activities and particularly:

Actor	Description	FCC Rules
SAS Administrator	Import FCC or Non-FCC databases	96.63 - b
SAS Administrator	Update SAS Software	

These two services are detailed in the next sections.

5.1.3.1. Import FCC or Non-FCC databases

For the 3.5 GHz CBRS band service to run properly, it is important that the SAS is synchronized with FCC (see §3.2.3) or non-FCC (see §3.2.4) databases on a daily-basis.

To ensure this synchronization, the SAS Administrator implements two procedures:

- Updating periodic procedure

  Overnight at a set time, the SAS Administrator will connect to the corresponding databases, will retrieve the data and update its SAS databases. This will first be done manually, but it is anticipated that the SAS Administrator will study the possibility for performing this operation automatically afterwards.

- Updating procedure on request

  If, for any reason, the FCC or other entity wants an immediate updating of the SAS data, it can connect to the SAS web portal and register a new request (5.1.2.11).

  The processing will then be identical to the "Updating periodic procedure". This processing is described in the following use case.

The workflow for data updating is described below:

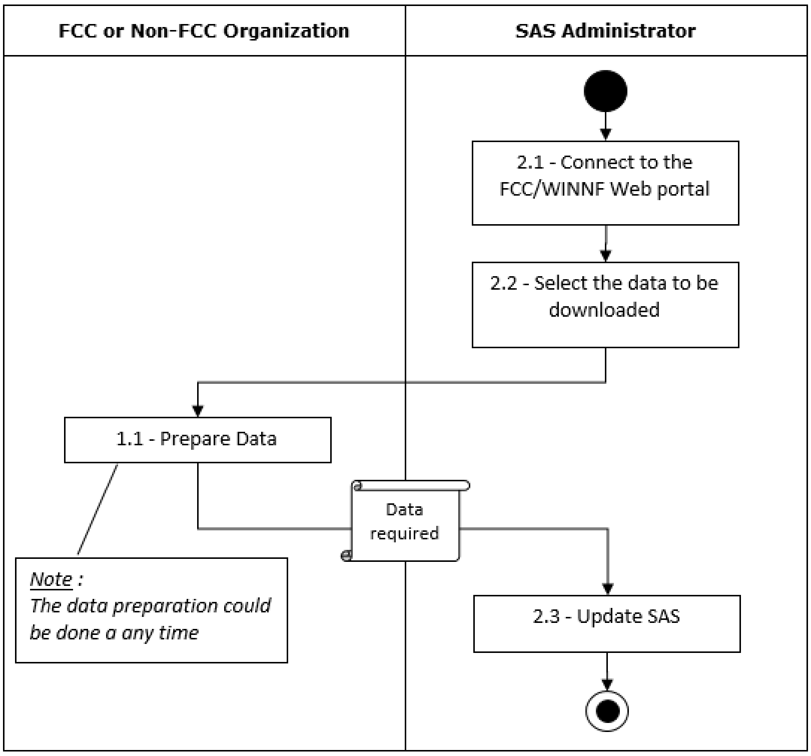

FCC or Non-FCC Organization
SAS Administrator
2.1 - Connect to the FCC/WINNF Web portal
2.2 - Select the data to be downloaded
1.1 - Prepare Data
Data required
Note :
The data preparation could be done a any time
2.3 - Update SAS

Figure 20: « Import Commission's databases» workflow

Step	Description
2.1	The SAS Administrator connects to the FCC or Non-FCC web portal
2.2	The SAS Administrator selects data and requests the download of this data
1.1	FCC or Non-FCC Web portal prepares the requested data
2.3	Once the data is downloaded, the SAS Administrator runs the updating data procedure to consider of the new data in the SAS

Table 12: « Import Commission's databases » workflow description

5.1.3.2. Software update

As the SASlive© is deployed in a cloud infrastructure (see §5.2.5), the SAS Administrator will benefit from the services of the cloud service provider for the installation and the updating of software.

5.1.3.2.1. Update the SAS web portals

The SAS administrator will use the *AWS Elastic Beanstalk* (see §5.2.5.1) to deploy, manage and scale the SAS web portals on servers and will follow the following AWS related procedures:

- Launch an application with AWS Elastic Beanstalk (https://aws.amazon.com/getting-started/tutorials/launch-an-app/)
- Update your Elastic Beanstalk App (see https://aws.amazon.com/getting-started/tutorials/update-an-app)

5.1.3.2.2. Update the SAS

For updating the SAS, the SAS administrator follows the workflow hereafter:

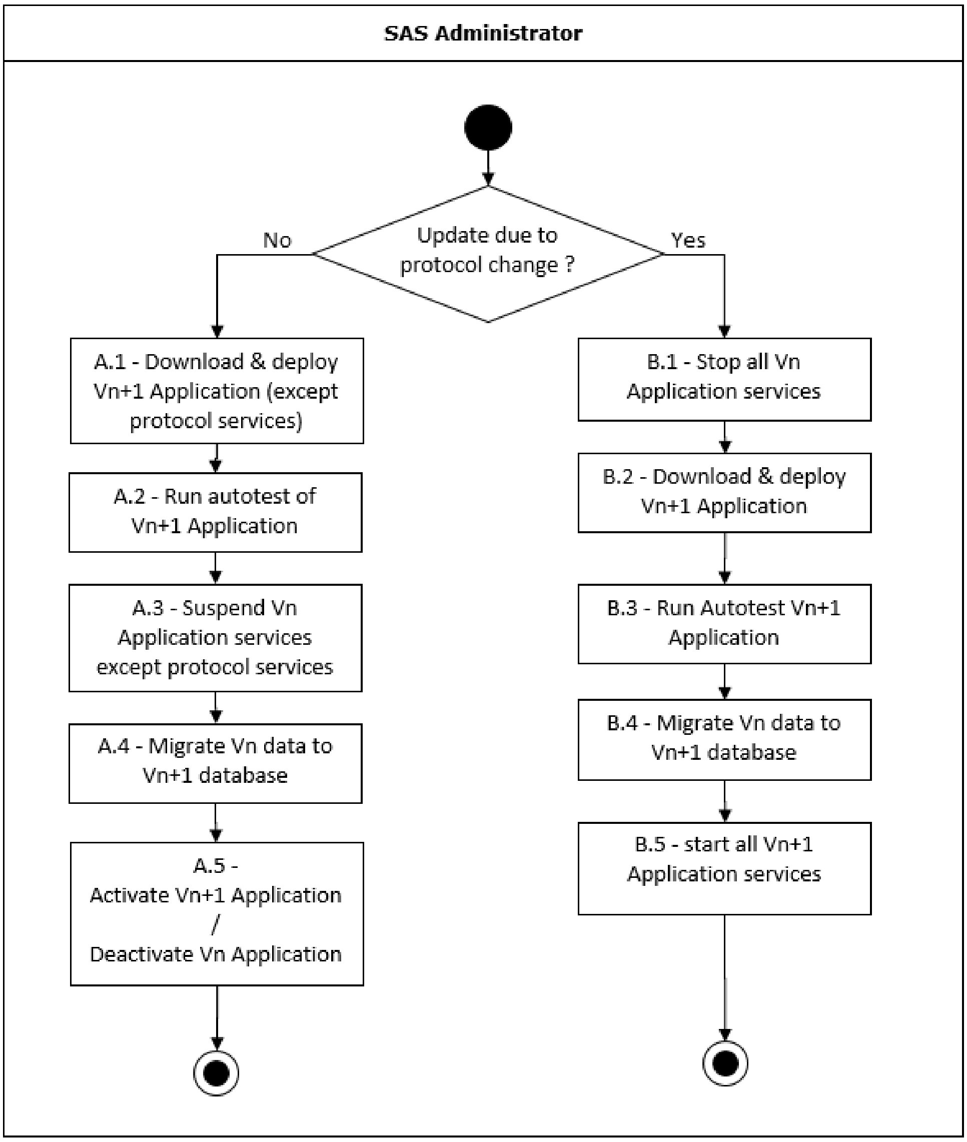

SAS Administrator
Update due to protocol change ?
No
Yes
A.1 - Download & deploy Vn+1 Application (except protocol services)
A.2 - Run autotest of Vn+1 Application
A.3 - Suspend Vn Application services except protocol services
A.4 - Migrate Vn data to Vn+1 database
A.5 - Activate Vn+1 Application / Deactivate Vn Application
B.1 - Stop all Vn Application services
B.2 - Download & deploy Vn+1 Application
B.3 - Run Autotest Vn+1 Application
B.4 - Migrate Vn data to Vn+1 database
B.5 - start all Vn+1 Application services

Figure 21: « Update SAS Software » workflow

Step	Description
A.1	If the update of the software is not due to an external interface change (SAS-SAS or SAS-CBSD or SAS-ESC) then only the part of the non-protocol application is updated. This is possible thanks to the modular architecture of the SASlive© which isolates the protocol aspect from the other parts (see Figure 22: SASlive© product architecture). In this case, the SAS Administrator downloads then deploys the new version (Vn+1) of the application (except protocol services) on the current virtual machine.
A.2	Once the application is downloaded and deployed, the SAS administrator runs the auto-tests to verify that the application has been successfully loaded. If the auto-test failed, the updating procedure is cancelled
A.3	The SAS administrator suspends the services of the *Vn* application. Note: During the suspension of these services, the protocol module no longer transmits any indications to the rest of the application and keeps them internally. But if this module receives a notification from the ESC, then the suspension of the services is canceled to process the notification from the ESC in high priority. The updating procedure is cancelled
A.4	The SAS Administrator migrates the data of the application *Vn* into the environment of the application *Vn+1*.
A.5	SAS administrator activates the services of the application *Vn+1* and deactivates the services of the application *Vn*.
B.1	SAS administrator stops all application services.
B.2	The SAS Administrator downloads then deploys the new version (*Vn+1*) of the application.
B.3	Once the application is downloaded and deployed, the SAS administrator runs the auto-tests to verify that the application has been successfully loaded
B.4	The SAS Administrator migrates the data of the application *Vn* into the environment of the application *Vn+1*
B.5	SAS administrator starts the services of the application.

Table 13: « Update SAS Software » workflow description

Note:

The downloaded application is signed.

5.2. SAS PRODUCT (SASLIVE©)

5.2.1. SASlive© product description

5.2.1.1. Architecture

The SASlive© product is divided into three sub-systems:

- The SAS web-portals:
  - This is the front end sub-system from which a user can connect to the SAS and request services described in the section §5.1.1.4,
- The SAS Ticketing tool:
  - This is the subsystem where user requests are logged before being processed by the SAS Administrator staff,
- The SAS:
  - This is the back-end sub-system that performs the core feature of the SASlive© product.

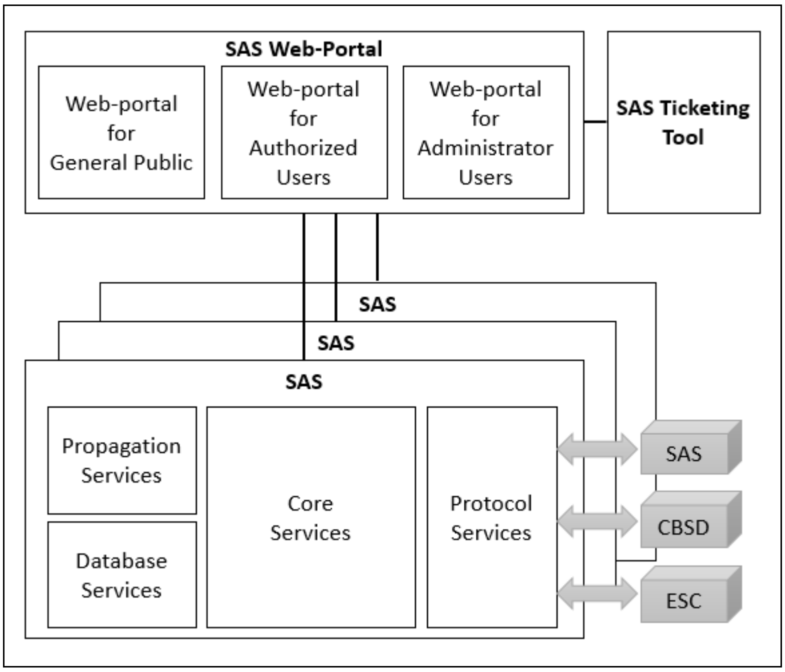


Figure 22: SASlive© product architecture

The next sections describe these three subsystems.

5.2.1.2. SAS web portals sub-system

5.2.1.2.1. Description

SASlive© offers a web-based Graphical User Interface for users who want to access to SAS information.

RED Technologies provides three different web portals according the target users:

- *SAS web-portal for general public*:
  - This portal provides free public data for the general public.
- *SAS web-portal for authorized users*:
  - This portal provides private access for authorized Commission (FCC) personnel, Federal incumbents, FSS incumbents, wireless broadband incumbents and CBSDs providers (SAS subscribers) and CPIs.
- *SAS web portal for administrator users*:
  - This portal provides access to RED Technologies staff for administration, maintenance and monitoring of the SAS.

Each web portal offers a specific list of services which vary in accordance with the profile and the level of confidentiality of the user (cf. §5.2.1.2.2).

5.2.1.2.2. Security Management

To ensure security of data access and visualization from the web portal, RED Technologies defines user's profiles:

- RED Technologies SAS Administrator staff,
- US President of the United States, or another designated Federal Government entity
- Authorized Commission (FCC) personnel,
- Federal incumbent,
- FSS Incumbent,
- Grandfathered wireless broadband incumbent,
- CBSDs authorized user (SAS subscribers)
- CPIs, (Certified professional installer)
- Other SAS Administrators
- General public.

These profiles are used to define different degrees of access to the information.

Any user (except the general public who has the lowest right, and access to public data only) must authenticate with his/her login and password to access the information given to him/her by his profile.

These profiles, login and password, are stored and encrypted within the database which in turn is stored in the Amazon Web Services (AWS) for security purposes.

The association of dedicated web portals and user profiles guarantees that a user will only have access to the information that concerns him/her, neither more nor less.

5.2.1.3. SAS ticketing tool sub-system

To trace the service requests submitted by the SAS Administrator's users, service requests are registered into a ticketing tool, called the **SAS ticketing tool**

The SAS ticketing tool is not accessible to external users, but a gateway allows for the transfer of data between the web portals and the SAS ticketing tool.

Each request will be processed according to the following workflow:

Status of the request	Description of the status
New	New request, just registered into the SAS ticketing tool
Feedback	The request requires more information from the user
Assigned	Assigned to SAS Administrator staff for processing
Done	The request is completed
Close	The user has been notified

Table 14: Workflow of a request logged in the SAS ticketing tool

Thanks to a 24/7 service center, RED Technologies guarantees that each request that is registered in the SAS ticketing tool will be processed as soon as possible at any time of the day or night.

Moreover, the implementation of the SLA indicators (e.g. the number of requests, their processing time) will allow RED Technologies to control the quality of the delivered SAS Administrator service. This means that RED Technologies will be able to adapt the size of its team according to estimated workload and the number of requests.

Lastly, the classification of requests according to three priority levels (high, medium, low) and by request issuer (U.S. President, Federal government entity, FCC, Licensee, CPI) enables them to be treated in line with their level of importance and not their level of arrival.

5.2.1.4. SAS sub-system

The diagram below describes the SAS architecture:

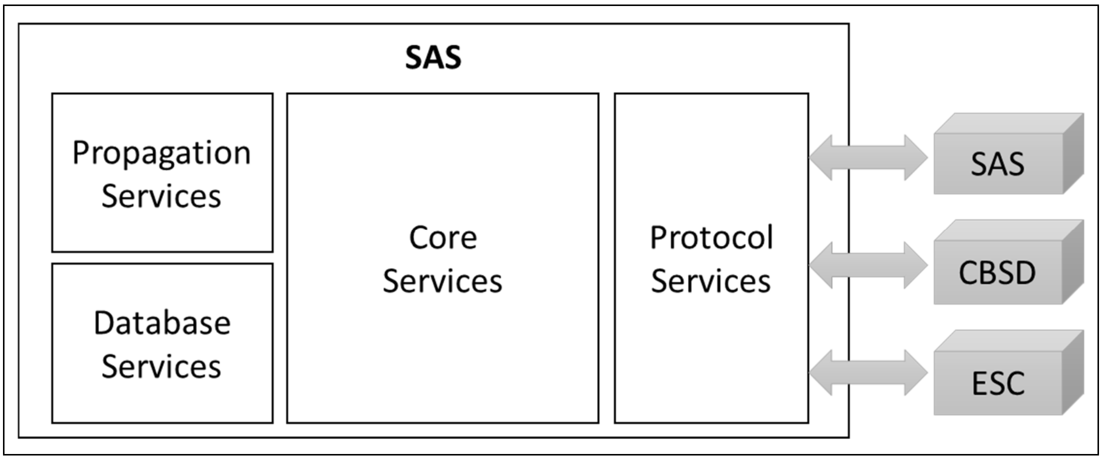


Figure 23: SAS architecture

The next section details the main services provided by the SAS.

5.2.1.4.1. Propagation Services

This service is dedicated to computing radio propagation. It implements, the propagation algorithms recommended by the Wireless Innovation Forum.

- For PPA calculation, PPA protection, and Grandfathered 3650-3700 MHz Band Licensees, it implements the NTIA model, with the modifications provided in 3.5 GHz CBRS band operational and functional requirements (see [Ref. 08]).
- For FSS earth stations and ESC sensor protection, it implements the NTIA ITS Irregular Terrain Model (ITM) implementation, in point-to-point mode, of the Longley-Rice propagation model.

5.2.1.4.2. Database services

This service provides secure data storage, secure data deletion and data access control to other services of the SASlive© product architecture.

Data is stored in SQL databases.

The following data is stored for SAS operation:

- A REM that stores the estimated received signal strengths of CBSDs emissions according to location,
- Data related to the deployment of incumbent sites, including:
  - FSS earth stations,
  - Federal sites,
  - Grandfathered wireless protection zones.
- PAL licenses,
- PPAs,
- CBSDs,
- Certificates,
- Events logs (such as events related to CBSD operation),
- Reports.

5.2.1.4.2.1.Long-term storage

Records not pertaining to federal incumbent user transmissions are archived in long-term storages, for a minimum of 60 months.

5.2.1.4.2.2.Certificates

The SAS stores a “SAS provider certificate” signed by a SAS Provider CA generating certificates according to the certificate policy specified in [Ref. 12]. This certificate enables entities connecting to the SAS (such as CBSDs, SASs, ESCs) to authenticate the SAS.

This “SAS provider certificate” is renewed every 15 months. It is formatted as an X.509 certificate and includes X.509 extensions specified in [Ref. 10].

In addition, the SAS maintains an up-to-date list of blacklisted CBSD certificates.

5.2.1.4.2.3.Security

Access to data is controlled by authentication and encryption algorithms to ensure that only authorized users can read or write data.

These security features are used to guarantee confidentiality of SAS Essential Data as defined in 3.5 GHz CBRS band operational and functional requirements (see [Ref. 08]).

A secure deletion feature ensures that critical information is reliably deleted from the system whenever requested.

This security feature is used when deleting records related to incumbent detection events provided by an ESC.

In addition, it will be ensured that:

- No element of the SASlive© product architecture has any connectivity to any military or sensitive federal databases or systems, unless required by the FCC for normal SAS operation.
- No element of the SASlive© product architecture stores, retains, transmits, or discloses any operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by the FCC to effectively operate the SAS.

5.2.1.4.3. Core Services

This service is responsible for fulfilling the following main SAS functions:

- Maintaining the state machines of each CBSD and each grant,
- Registering and validating PPAs,
- Determining and providing to CBSDs the permissible channels and maximum permissible transmission power level in the most optimal manner, while protecting Tier 1 and Tier 2.

5.2.1.4.3.1.CBSD control

The core service maintains:

- One registration state machine for each CBSD, and
- One grant state machine for each grant for a given CBSD.

CBSD registration state machine:

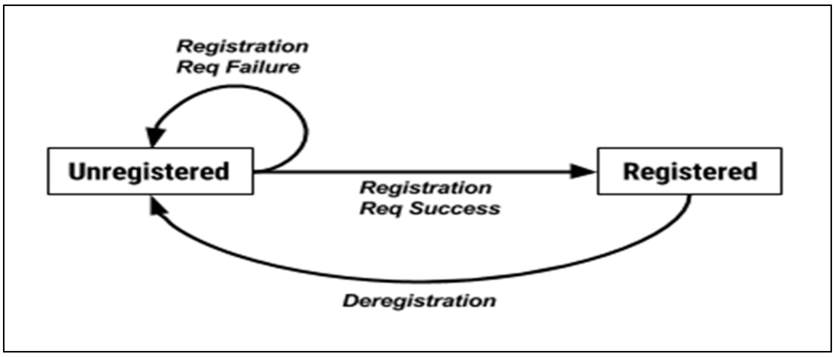


Figure 24: CBSD Registration state machine

Upon registering a CBSD, the core service verifies that the parameters provided in the registration are valid (including the FCC Identification number, to ensure that the CBSD is a certified device), according to [Ref. 07].

If no exchange is performed between the SAS and a CBSD for seven days, the core service moves this CBSD to the "unregistered" state.

CBSD grant state machine:

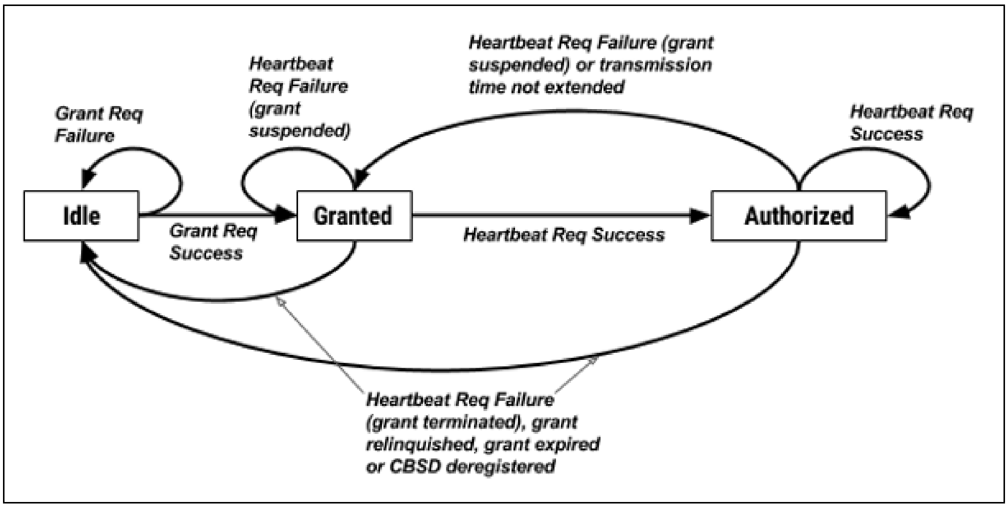

Grant Req Failure
Heartbeat Req Failure (grant suspended)
Heartbeat Req Failure (grant suspended) or transmission time not extended
Heartbeat Req Success
Idle
Granted
Authorized
Grant Req Success
Heartbeat Req Success
Heartbeat Req Failure (grant terminated), grant relinquished, grant expired or CBSD deregistered

Figure 25: CBSD grant state machine

Every time a grant request is received from a registered CBSD, the core service instantiates a new CBSD grant state machine.

Channels for a given grant are identified by the core service as described in §5.2.1.4.3.4.

5.2.1.4.3.2. Radio Environment Map (REM)

The REM stores the estimated Received Signal Strength (RSS) of CBSDs emissions according to their location and transmission parameters.

It is used to:

- Protect Tier 1 and Tier 2, and minimize interference when allocating channels (see §5.2.1.4.3.4),
- Optimize channel allocation among CBSDs while ensuring fairness and coexistence among multiple radio access technologies.
- Resolve interference upon receiving interference reports.
- Visualize estimated coverage of CBSDs (e.g. to aid during network planning).

Furthermore the REM stores at each point to be protected (i.e., at a given latitude, longitude and height) the value of the RSS produced by each CBSDs, for each 10MHz frequency range on which a grant is active.

This RSS value associated with a CBSD considers the CBSD conducted transmission mask, according to the maximum allowed CBSD Out of Band Emission (OOBE).

The REM allows the availability, for each location, of the following information:

- The total aggregated RSS,
- The list of CBSDs and their estimated RSS.

This data can be visualized through a GIS to resolve interferences, and to identify the CBSDs that are potentially causing those interferences.

5.2.1.4.3.3.PPA registration and validation

This core service is responsible for handling PPA registration and ensuring that the PPA contour provided is contained within the calculated PPA contour.

A. PPA contour calculation

The coverage of each registered CBSD, up to a threshold of -96dBm / 10MHz, is determined using the REM.

The maximum allowed contour of the PPA will be determined following the methodology as defined by the Wireless Innovation Forum, based on the coverage of each registered CBSD.

B. PPA restrictions validation

When registering a new PPA, the core service ensures that no PAL holder has registered more than four frequencies at the same location, based on the list of PPAs and the list of PAL licenses stored within the database service.

The core service also verifies that the provided PPA contour doesn’t overlap with areas on which the PAL holder doesn’t own any PAL license.

5.2.1.4.3.4.Channel allocation

Before indicating to a CBSD that a channel is available (e.g. following a spectrum inquiry request), or granting a channel to a CBSD (e.g. following a spectrum grant request), the core service performs the following main tasks:

A. Validation of the parameters,

B. Protection of Tier 1 and Tier 2,

C. Interference mitigation and optimization.

For GAA channels the core services will identify channels from 3550 to 3700 MHz.

For PAL channels, the core services will identify channels from 3550 to 3650 MHz.

Those tasks are described in more details in the following subsections.

A. Validation of the parameters

If no ESC is deployed, the core service considers that no channel is available for Category B CBSDs and that Category A CBSDs are authorized only outside of exclusion zones.

The core service also ensures that the following limitations on CBSD transmission power are satisfied:

- For CBSDs registered as category A, the maximum allowed EIRP is not above 30dBm on each 10MHz channel.
- For CBSDs registered as category B, the maximum allowed EIRP is not above 47dBm on each 10MHz channel.

B. Protection of Tier 1 and Tier 2

The core service ensures that the following protections are met:

- ESC protection,
- Federal sites protection,
- FSS protection,
- Grandfathered Wireless Broadband Licensees protection,

- PPA protection.

To protect Tier 1 and Tier 2, the aggregated interference of all registered CBSDs (including CBSDs registered in other SASs) is computed using the REM (see §5.2.1.4.3.2). The method used to compute aggregated interference follows the recommendations of the Wireless Innovation Forum (described in R2-SGN-12 of 3.5 GHz CBRS band operational and functional requirements, see [Ref. 08])

Further details on those protections are described in the following subsections.

B.1 ESC protection

The core service ensures that zones associated with incumbent detection events, provided by the ESC to SAS interface, are protected.

The following parameters are provided by the SAS – ESC interface:

- A geographic description of the federal incumbent activity to be protected,
- The frequency range of the federal incumbent activity to be protected,
- A protection level specifier to be enforced by the SAS, if provided by the partner ESC.

Once an incumbent detection event has expired and the retention time has expired, the core service is notified by the 'ESC to SAS interface' to securely delete all data stored within the database service associated with this event.

Within the 3550-3650 MHz band, if there are no sensors connected to an ESC deployed along the coastline, all grants requested by a category A CBSD located within an NTIA-defined exclusion zone along the coastline, or a category B CBSD anywhere are rejected by the core service.

Within the 3650-3700 MHz band, if there are no sensors connected to an ESC deployed at or near federal radiolocation sites listed in 47 CFR 90.1331 and 47 CFR 2.106, US 109, all grants requested by a category A or category B CBSD located within 80 km of the designated federal sites are rejected by the core service.

B.2 FSS protection

An up-to-date list of FSS sites is stored in the database service.

For grandfathered FSS operating in 3600-3700 MHz, the core service ensures that the following requirements are fulfilled:

Protection Scenario	Protection Criteria
3600-3700 MHz FSS Co-Channel Protection	The aggregate passband RF power spectral density at the output of a reference RF filter and antenna at the location of an FSS earth station operating in the 3600 – 3700 MHz band, produced by emissions from all co-channel CBSDs (within 150 km) operating in the 3.5 GHz CBRS band shall not exceed a median RMS value of -129dBm / MHz.
3600-3700 MHz FSS Blocking Protection	The aggregate RF power at the output of a reference RF filter and antenna at the location of an FSS earth station operating in the 3600 – 3700 MHz band, produced by emissions from all CBSDs (within 40 km), shall not exceed a median RMS value of -60dBm.
Protection of FSS in 3650-3700 MHz with Grandfathered Wireless Broadband Licensees in the Protection Area	SAS needs to protect grandfathered FSS earth stations in the 3650-3700 MHz band based on part 90, subpart Z. If there is at least one valid GWBL license within a 150 kms radius centered at the FSS earth station, no CBSD can operate within 150 km of the FSS earth station.

Table 15: Protection criteria (3600-3700 MHz)

For grandfathered FSS operating in 3700-4200 MHz, the core services ensure that the following requirements are fulfilled:

Protection Scenario	Protection Criteria
Protection of Out-of-Band Emission into 3700-4200MHz TT&C FSS	The aggregate passband RF power spectral density at the output of a reference RF filter and antenna at the location of a TT&C FSS earth station operating in the 3700 – 4200 MHz band, produced by emissions from all CBSDs (within 40 km) operating in the Citizens Band Radio Service shall not exceed a median RMS value of -129dBm / MHz.
3700-4200 MHz TT&C FSS Blocking Protection	The aggregate RF power at the output of a reference RF filter and antenna at the location of a TT&C FSS earth station operating in the 3700 – 4200 MHz band, produced by emissions from all CBSDs (within 40 km), shall not exceed a median RMS value of -60dBm.

Table 16: Protection criteria (3700-4200MHz)

B.3 Grandfathered Wireless Broadband Licensees protection

An up-to-date list of registered Grandfathered Wireless Broadband Licensees protection zones is maintained by the database service.

At each point inside each grandfathered wireless protection zone, the core services verifies, using the REM, that the aggregate power of all CBSDs is not greater than -80dBm / 10MHz.

B.4 PPA protection

An up-to-date list of registered PPAs is maintained by the database service.

At each point inside each PPA, the core service verifies, using the REM, that the aggregate power of all CBSDs (not including the CBSDs registered in this PPA) is not greater than -80dBm / 10MHz.

C. Interference mitigation and channel selection optimization

C.1 Channel contiguity

PAL channel assignments are assumed to be pre-determined and shared in a PAL database, according to Wireless Innovation Forum Release 1. Enhancements may be specified in future releases and SASlive© will be updated accordingly (see latest Wireless Innovation Forum roadmap [Ref. 15])

Whenever feasible, it is assumed that pre-determined PAL channels are identical for geographically contiguous areas held by the same Priority Access Licensee.

Whenever feasible, it is also assumed that pre-determined PAL channels are identical for contiguous frequencies within the same license area held by the same Priority Access Licensee.

C.2 Channel selection

When multiple frequencies are identified as available, the core service uses the REM to select the most optimal channel(s), according to the following steps:

- Identifying overlapping coverage areas among registered CBDS, and,
- Granting different channels, if possible non-contiguous, to CBSDs whose coverage is overlapping.

Note:

> Some types of optimization that will be performed by the core service depend on technical topics that are still being discussed within the Wireless Innovation Forum, including:

- The types of parameters provided within a grant request or a spectrum inquiry request (for example a specific range of frequencies or a bandwidth),
- Mechanisms to enable fairness and coexistence among CBSDs.

5.2.1.4.4. Protocol Services

5.2.1.4.4.1.CBSD – SAS interface

This interface implements the SAS to CBSD protocol as defined in [Ref. 07]. This interface is secured using the TLS protocol (see [Ref. 10]).

The CBSD – SAS interface receives Registration, Spectrum Inquiry, Grant, Heartbeat and Deregistration requests from CBSDs or from Domain Proxies, and replies to those requests as specified in the SAS to CBSD protocol, after interacting with the SAS core service whenever necessary.

The interactions between the CBSD-SAS interface and the core service can be summarized as follows:

- Upon receiving a Registration request, it requests the core service to validate and store parameters of this CBSD within the database service.
- Upon receiving a Spectrum Inquiry request, it requests the core service to identify available channels, among those provided in the request, and to provide the result in a Spectrum Inquiry Response.
- Upon receiving a Grant request, it requests the core service to validate whether the requesting CBSD can be allowed to transmit according to the provided parameters and to identify alternative parameters if the request cannot be accepted. It then provides the result in a Spectrum Inquiry Response.
- Upon receiving a Heartbeat request for a given grant, it requests the core service to validate whether the CBSD associated with this grant is still allowed to transmit according to the parameters of this grant, and provides the result in a Heartbeat Response.
- Upon receiving a Deregistration request, it requests the core service to update the status of this CBSD and its associated grants.

5.2.1.4.4.2.SAS – SAS Interface

This interface implements the SAS to SAS protocol as specified in [Ref. 06]. This interface is secured using the TLS protocol (see [Ref. 10]).

The following data will be synchronized with other authorized SAS, and will follow WInnF conclusions regarding timing requirements:

- CBSD physical installation parameters,
- CBSD coexistence parameters (e.g. interference coordination group memberships, air interface standards),
- Information on CBSD grants: CBSD grant information (frequency ranges), power, grant type, grant expiration time, requested authorization status (Priority Access or General Authorized Access)
- PAL Protection Area (PPA) records,
- SAS-SAS coordination event records.

Data received from other SAS will be stored in the database service.

5.2.1.4.4.3.SAS – ESC Interface

The interface between this module and the approved ESC may vary according to the ESC vendor and will be adapted accordingly.

RED Technologies is in contact with prospective ESC operators and will work with them to jointly define a fully functional and secure SAS-ESC interface (see §3.2.6).

5.2.2. SASlive© development and test process

The SASlive© product is developed in accordance with the Project Delivery Processes defined by RED Technologies for Internal Customer Process:

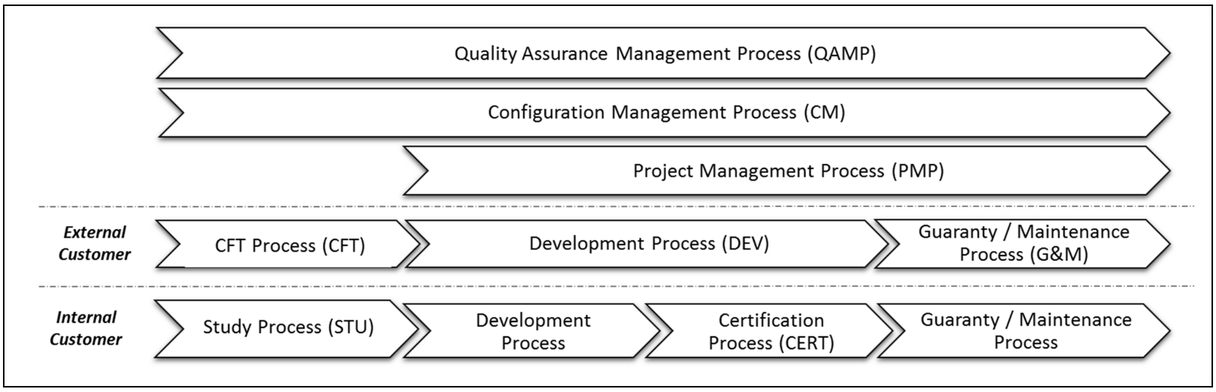

Quality Assurance Management Process (QAMP)
Configuration Management Process (CM)
Project Management Process (PMP)
External Customer
CFT Process (CFT)
Development Process (DEV)
Guaranty / Maintenance Process (G&M)
Internal Customer
Study Process (STU)
Development Process
Certification Process (CERT)
Guaranty / Maintenance Process

Figure 26: RED Technologies Project Delivery Process

This Development Process is based on an incremental V-cycle model and on best practices from Capability Maturity Model Integration (CMMI).

The SASlive© is developed in C# with .Net framework and in C in accordance with software development process defined by RED Technologies.

Redmine is used for feature planning, documentation and bug tracking management whereas configuration management is performed with *Git* for code and *TortoiseSVN* for documentation.

To check that the software meets the requirements, several verifications are performed during the development cycle. These verifications include:

- Specifications and technical documents reviews,
- Tests (unit, integration and validation),
- Sampling code audits.

In addition, RED Technologies will internally replicate the certification platform and will perform the tests defined by WInnF - SSC Work Group 4 (Test and Certification) (see [Ref. 09]).

5.2.3. SASlive© interoperability testing (IOT)

To verify and to prove the multi-vendor compatibility of its SAS, RED Technologies is performing Interoperability Tests with several CBSDs and SAS providers.

On April 2017, RED Technologies and Ruckus Wireless Complete Interoperability Tests to Enable Advanced Wireless Services Using CBRS and Future 5G Spectrum Sharing (see press release §6.5).

In addition, RED Technologies plans to conduct IOT tests with ESC operators. (cf. §3.2.6)

5.2.4. SASlive© certification

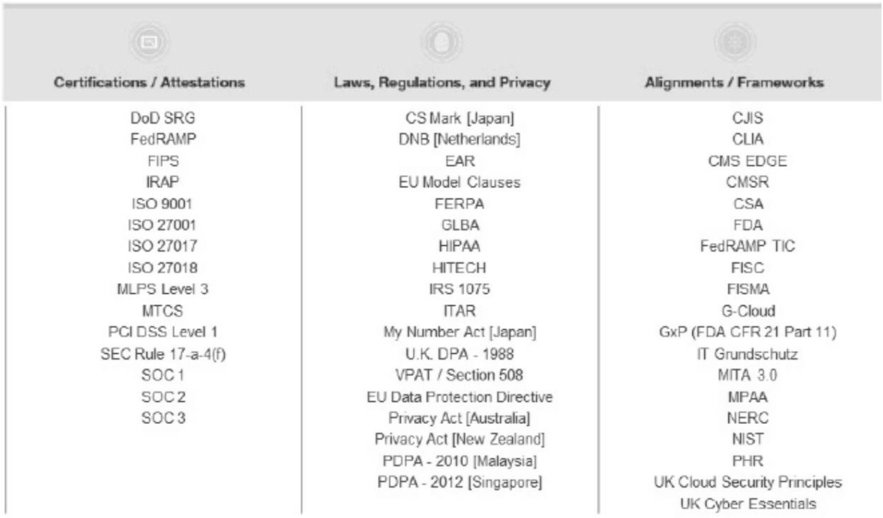
RED Technologies will follow the test and certification process as defined by [Ref. 09].

RED Technologies participates in the definition and development of the tests which help to certify the SAS as part of its participation in SSC Work Group 4 (Test and Certification).

5.2.5. SASlive© deployment

RED Technologies will deploy its SASlive© product in a cloud environment. After the study of several service providers, **RED Technologies selected Amazon Web Services (AWS),** to host its SASlive©, for the following main reasons:

- AWS provides a lot of services and tools for computing, storage, database, networking, security.
- **Data is hosted on US territory (Oregon, California, Virginia, and Ohio).**
- AWS IT infrastructure is designed and managed in alignment with the best security practices and a variety of IT security standards:



Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
DoD SRG	CS Mark [Japan]	CJIS
FedRAMP	DNB [Netherlands]	CLIA
FIPS	EAR	CMS EDGE
IRAP	EU Model Clauses	CMSR
ISO 9001	FERPA	CSA
ISO 27001	GLBA	FDA
ISO 27017	HIPAA	FedRAMP TIC
ISO 27018	HITECH	FISC
MLPS Level 3	IRS 1075	FISMA
MTCS	ITAR	G-Cloud
PCI DSS Level 1	My Number Act [Japan]	GxP (FDA CFR 21 Part 11)
SEC Rule 17-a-4(f)	U.K. DPA - 1988	IT Grundschutz
SOC 1	VPAT / Section 508	MITA 3.0
SOC 2	EU Data Protection Directive	MPAA
SOC 3	Privacy Act [Australia]	NERC
	Privacy Act [New Zealand]	NIST
	PDPA - 2010 [Malaysia]	PHR
	PDPA - 2012 [Singapore]	UK Cloud Security Principles
		UK Cyber Essentials

AWS Source: see https://aws.amazon.com/compliance/resources/.

Figure 27: Best security practices and IT security standards of AWS

RED Technologies will use several services provided by AWS that can be classified in three groups:

- Compute & Network management
- Database management
- Security management

5.2.5.1. Compute & Network management

For network management, the SASlive© will use:

- *AWS Virtual Private Cloud*: to isolate different parts of the SASlive© (e.g. SAS Web portal and SAS) and manage security access,
- *AWS Elastic Load Balancing*: to perform load balancing between different servers and to enable fault tolerance mechanisms,
- *AWS Elastic Beanstalk*: to deploy, manage and scale SAS web portal and SAS.

5.2.5.2. Database management

Amazon RDS is used to handle the database and provides access to specific features:

- *Easy Storage Scaling*: this feature allows for growing the size of the SAS database volume as database storage needs increase,
- *Automated Backups*: this feature enables point-in-time recovery for a SAS database instance,
- *Automatic Host Replacement*: this feature allows for the replacement of the compute instance powering SAS deployment in the event of a hardware failure,

- *Data Encryption*: this feature allows for the encryption of SAS databases using keys,
- *Monitoring and Metrics*: this feature allows the handling of operational metrics for database instances, including compute, memory, storage, query throughput, cache hit ratio, and active connections.

5.2.5.3. Security management

For security management, the SASlive© will be based on:

- *AWS Identity & Access Management*: to securely control access to AWS services and resources,
- *AWS Certificate Manager*: to manage and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. These certificates are used to secure all network communications and establish the identity of websites over the internet,
- *AWS Key Management Service*: to create and control the encryption keys used to encrypt data,
- *AWS WAF*: AWS firewall to protect servers from external attacks.

Moreover, RED Technologies will use *AWS Inspector* which is an automated security assessment service that helps to improve the security and compliance of applications deployed on AWS.

6. APPENDIX

6.1. DOCUMENTATION REFERENCE

Ref	Title	Source	Reference
[Ref. 01]	PUBLIC NOTICE Wireless Telecommunications Bureau and Office of Engineering and Technology Establish Procedure and Deadline for Filing Spectrum Access System (SAS) Administrator(s) and Environmental Sensing Capability (ESC) Operator(s) Applications GN Docket No. 15-319	FCC	DA 15-1426 Released: December 16, 2015
[Ref. 02]	PUBLIC NOTICE WIRELESS TELECOMMUNICATIONS BUREAU AND OFFICE OF ENGINEERING AND TECHNOLOGY CONDITIONALLY APPROVE SEVEN SPECTRUM ACCESS SYSTEM ADMINISTRATORS FOR THE 3.5 GHZ BAND	FCC	DA 16-1426 Released: December 21, 2016
[Ref. 03]	PUBLIC NOTICE WIRELESS TELECOMMUNICATIONS BUREAU AND OFFICE OF ENGINEERING AND TECHNOLOGY ESTABLISH “SECOND WAVE” DEADLINE FOR PROPOSALS FROM PROSPECTIVE SPECTRUM ACCESS SYSTEM (SAS) ADMINISTRATOR(S) ANDENVIRONMENTAL SENSING CAPABILITY (ESC) OPERATOR(S) GN Docket No. 15-319	FCC	DA 17-339 Released: April 7, 2017
[Ref. 04]	Federal Communications Commission - FCC 15-47 REPORT AND ORDER AND SECOND FURTHER NOTICE OF PROPOSED RULEMAKING GN Docket No. 12-354	FCC	Released: April 21, 2015
[Ref. 05]	Federal Communications Commission - FCC 16-55 ORDER ON RECONSIDERATION AND SECOND REPORT AND ORDER GN Docket No. 12-354	FCC	Released: May 2, 2016
[Ref. 06]	Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - SAS Interface Technical Specification Document WINNF-16-S-0096	WInnF (WG3)	Release 1
[Ref. 07]	Signaling Protocols and Procedures for Citizens Broadband Radio Service (CBRS): Spectrum Access System (SAS) - Citizens Broadband Radio Service Device (CBSD) Interface Technical Specification Document WINNF-16-S-0016	WInnF (WG3)	Release 1
[Ref. 08]	Requirements for Commercial Operation in the U.S. 3550-3700 MHz Citizens Broadband Radio Service Band Document WINNF-15-S-0112	WInnF (WG1)	Release 1
[Ref. 09]	Test and Certification for Citizens Broadband Radio Service (CBRS); Conformance and Performance Test	WInnF	Release 1

	Technical Specification; SAS as Unit Under Test (UUT) Document WINNF-15-S-0061	(WG4)	
[Ref. 10]	CBRS Communications Security Technical Specification Document WINNF-15-S-0065	WInnF (WG2)	Release 1
[Ref. 11]	CBRS Operational Security Technical Specification Document WINNF-15-S-0071	WInnF (WG2)	Release 1
[Ref. 12]	WInnForum CBRS Certificate Policy Specification Document WINNF-17-S-0022	WInnF (WG5)	Release 1
[Ref. 13]	Operations for Citizens Broadband Radio Service (CBRS): Priority Access License (PAL) Database Technical Specification Document WINNF-16-S-0245	WInnF (WG5)	Release 1
[Ref. 14]	CBRS Certified Professional Installer Accreditation Technical Specification Document WINNF-16-S-0247	WInnF (WG5)	Release 1
[Ref. 15]	SPECTRUM SHARING COMMITTEE PROJECT ROADMAP	WInnF	April 4, 2017

Table 17: Documentation Reference

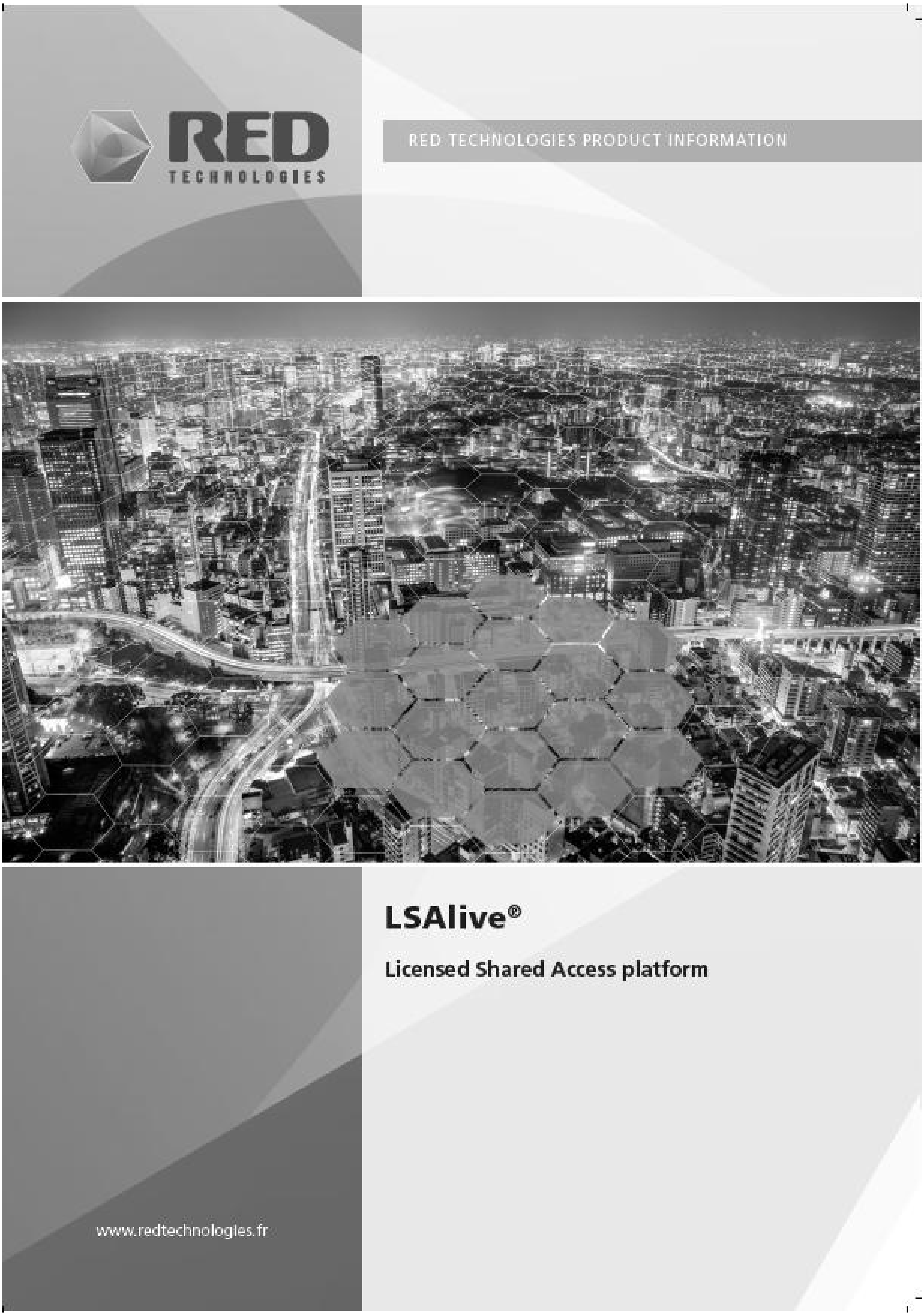
6.2. GLOSSARY

Terms	Description
3GPP	3rd Generation Partnership Project
AWS	Amazon Web Services
CA	Certificate Authority
CBSD	Citizens Broadband Radio Service Devices
CBRS	Citizens Broadband Radio Service
CFT	Call For Tender
CMMI	Capability Maturity Model Integration
CR	Cognitive Radio
CRAN	Cloud-RAN
DoD	Department of Defense
DP	Domain Proxy
EMS	Element Management System
ESC	Environmental Sensing Capability
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FSS	Commercial Fixed Satellite Service
GAA	General Authorized Access
GIS	Geographical Information System
GWBL	Grandfathered Wireless Broadband Licensee
IOT	Interoperability Testing
ITM	Irregular Terrain Model
ITS	Institute for Telecommunication Sciences
LAA	Licensed-Assisted Access
LSA	License-Shared Access
LSAlive©	RED Technologies License-Shared Access Product
LTE	Long Term Evolution
LTE-U	LTE Unlicensed
mmWave	millimeter Wave
MWC	Mobile World Congress
NTIA	National Telecommunications and Information Administration (regulator of U.S. federal government spectrum use)
OET	Office of Engineering and Technology
OOBE	Out Of Band Emission
PALs	Priority Access Licensees
RAN	Radio Access Network
REM	Radio Environment Map
RSS	Received Signal Strength
SAS	Spectrum Access System
SASlive©	RED Technologies Spectrum Access System Product
SDR	Software Defined Radio
SLA	Service Level Agreement
TT&C	Telemetry, Tracking, and Control
ULS	Universal Licensing System
WTB	Wireless Telecommunications Bureau
WInnF	Wireless Innovation Forum

Table 18: Glossary

6.3. COMPANY'S REFERENCE

6.3.1. LSAlive© Marketing Brochure



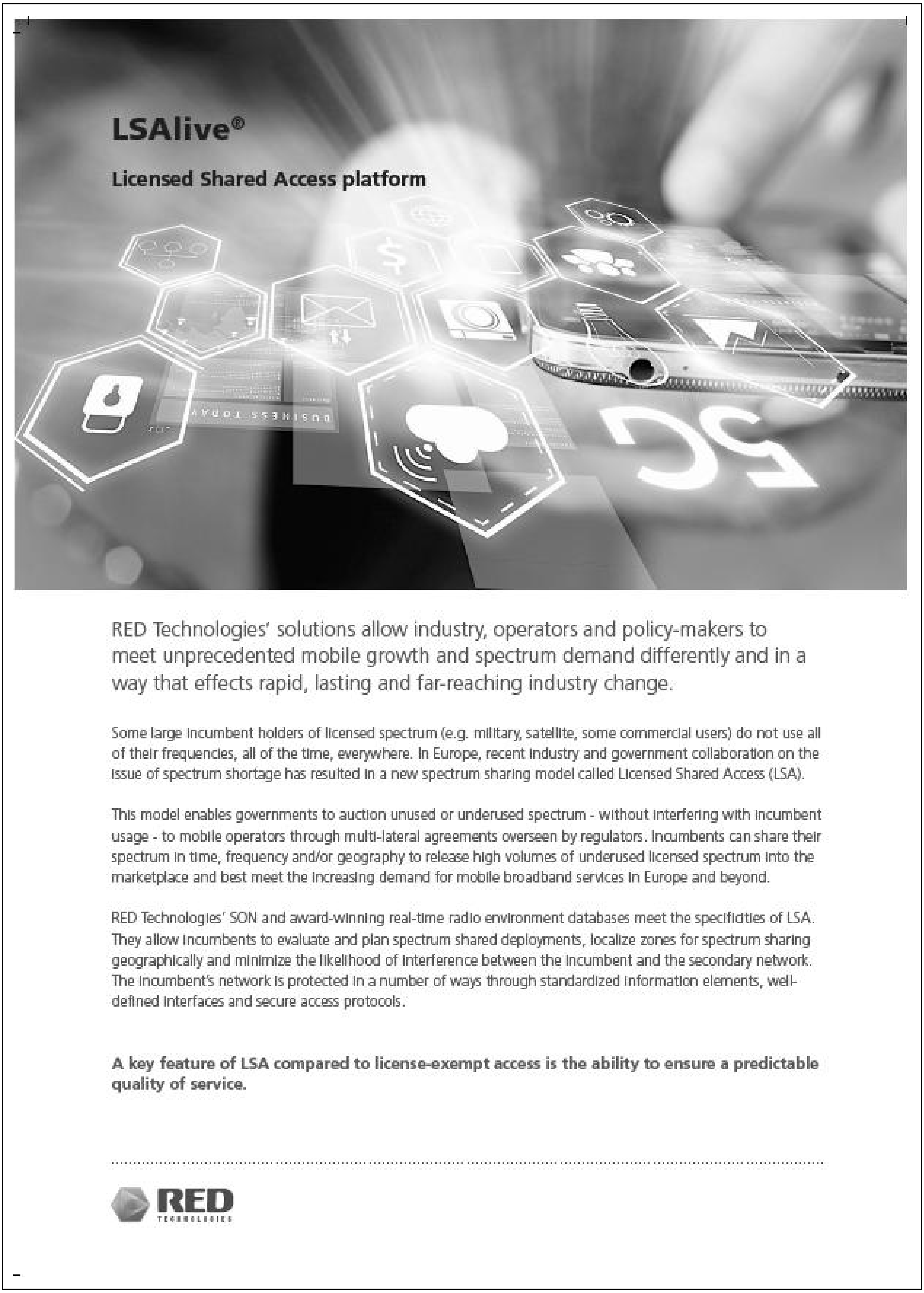
RED TECHNOLOGIES

RED TECHNOLOGIES PRODUCT INFORMATION

LSAlive®

Licensed Shared Access platform

www.redtechnologies.fr



LSAlive®

Licensed Shared Access platform

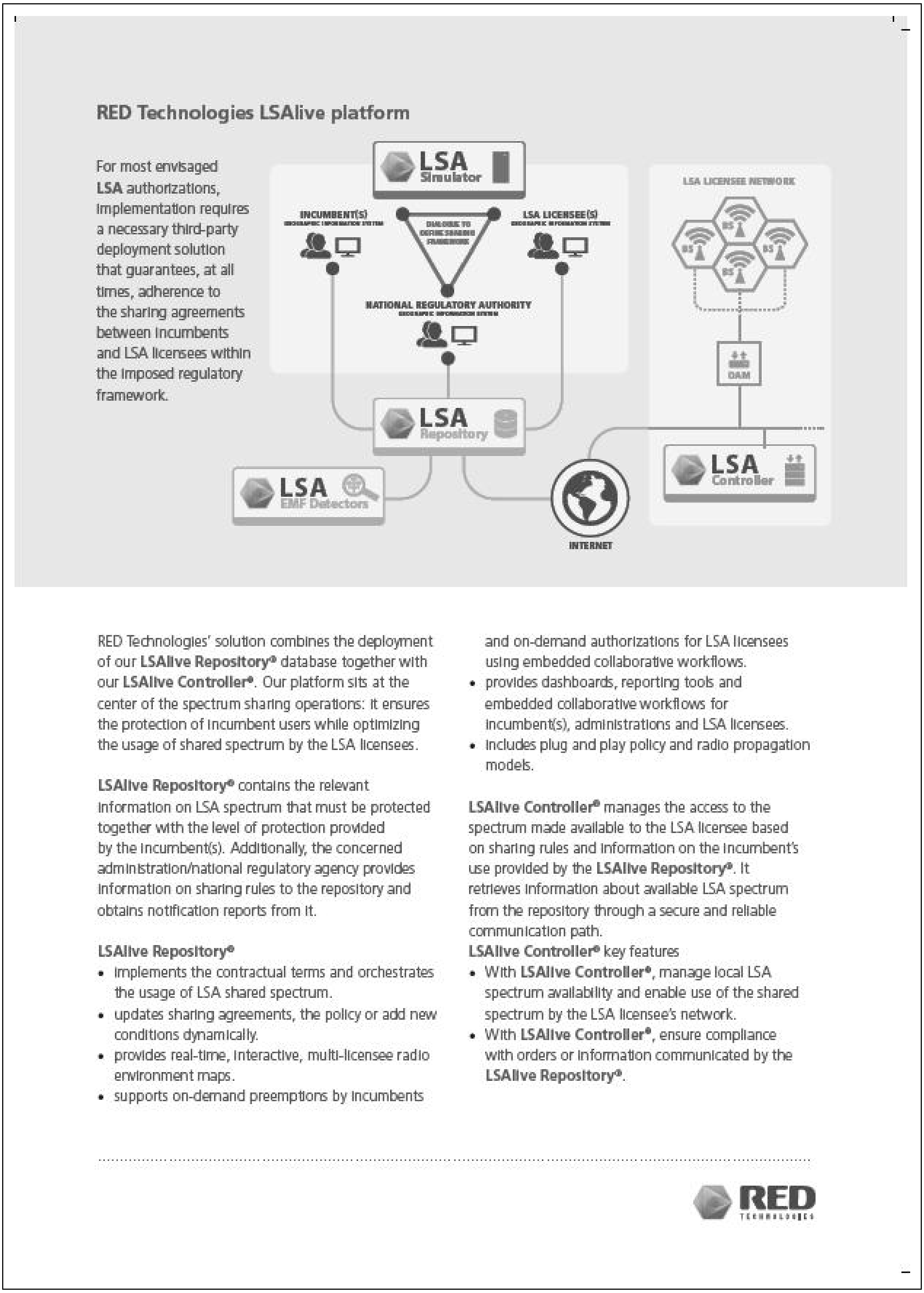
RED Technologies' solutions allow industry, operators and policy-makers to meet unprecedented mobile growth and spectrum demand differently and in a way that effects rapid, lasting and far-reaching industry change.

Some large incumbent holders of licensed spectrum (e.g. military, satellite, some commercial users) do not use all of their frequencies, all of the time, everywhere. In Europe, recent industry and government collaboration on the issue of spectrum shortage has resulted in a new spectrum sharing model called Licensed Shared Access (LSA).

This model enables governments to auction unused or underused spectrum - without interfering with incumbent usage - to mobile operators through multi-lateral agreements overseen by regulators. Incumbents can share their spectrum in time, frequency and/or geography to release high volumes of underused licensed spectrum into the marketplace and best meet the increasing demand for mobile broadband services in Europe and beyond.

RED Technologies' SON and award-winning real-time radio environment databases meet the specificities of LSA. They allow incumbents to evaluate and plan spectrum shared deployments, localize zones for spectrum sharing geographically and minimize the likelihood of interference between the incumbent and the secondary network. The incumbent's network is protected in a number of ways through standardized information elements, well-defined interfaces and secure access protocols.

A key feature of LSA compared to license-exempt access is the ability to ensure a predictable quality of service.


LSA Simulator
INCUMBENT(S)
GEOGRAPHIC INFORMATION SYSTEM
DIALOGUE TO DEFINE SHARING FRAMEWORK
LSA LICENSEE(S)
GEOGRAPHIC INFORMATION SYSTEM
NATIONAL REGULATORY AUTHORITY
GEOGRAPHIC INFORMATION SYSTEM
LSA LICENSEE NETWORK
BS
BS
BS
BS
OAM
LSA Repository
LSA EMF Detectors
INTERNET
LSA Controller
RED TECHNOLOGIES

RED Technologies LSAlive platform

For most envisaged **LSA** authorizations, implementation requires a necessary third-party deployment solution that guarantees, at all times, adherence to the sharing agreements between incumbents and LSA licensees within the imposed regulatory framework.

RED Technologies' solution combines the deployment of our **LSAlive Repository®** database together with our **LSAlive Controller®**. Our platform sits at the center of the spectrum sharing operations: it ensures the protection of incumbent users while optimizing the usage of shared spectrum by the LSA licensees.

LSAlive Repository® contains the relevant information on LSA spectrum that must be protected together with the level of protection provided by the incumbent(s). Additionally, the concerned administration/national regulatory agency provides information on sharing rules to the repository and obtains notification reports from it.

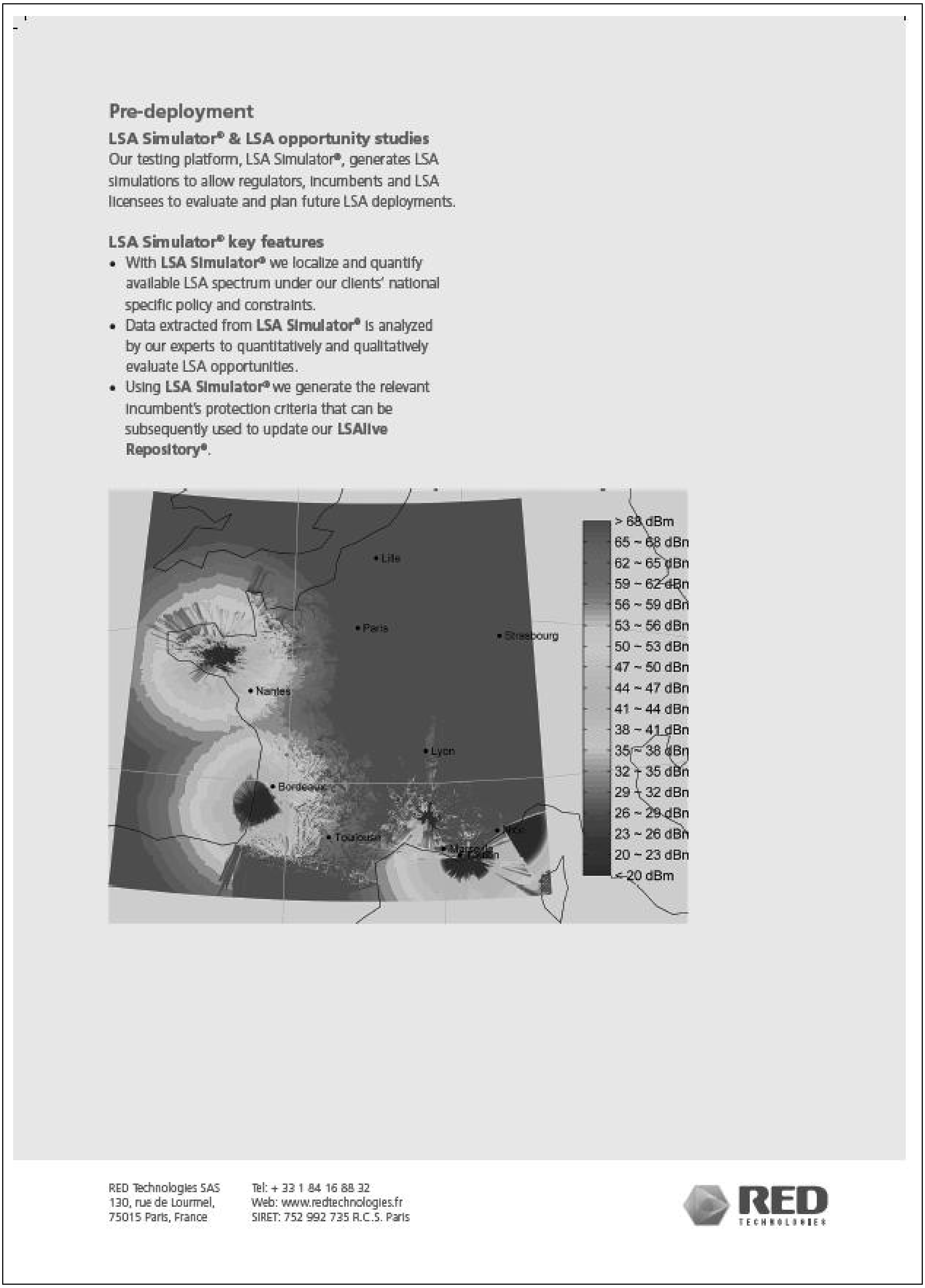
LSAlive Repository®

- implements the contractual terms and orchestrates the usage of LSA shared spectrum.
- updates sharing agreements, the policy or add new conditions dynamically.
- provides real-time, interactive, multi-licensee radio environment maps.
- supports on-demand preemptions by incumbents and on-demand authorizations for LSA licensees using embedded collaborative workflows.
- provides dashboards, reporting tools and embedded collaborative workflows for incumbent(s), administrations and LSA licensees.
- includes plug and play policy and radio propagation models.

LSAlive Controller® manages the access to the spectrum made available to the LSA licensee based on sharing rules and information on the incumbent's use provided by the **LSAlive Repository®**. It retrieves information about available LSA spectrum from the repository through a secure and reliable communication path.

LSAlive Controller® key features

- With **LSAlive Controller®**, manage local LSA spectrum availability and enable use of the shared spectrum by the LSA licensee's network.
- With **LSAlive Controller®**, ensure compliance with orders or information communicated by the **LSAlive Repository®**.



Pre-deployment

LSA Simulator® & LSA opportunity studies

Our testing platform, LSA Simulator®, generates LSA simulations to allow regulators, incumbents and LSA licensees to evaluate and plan future LSA deployments.

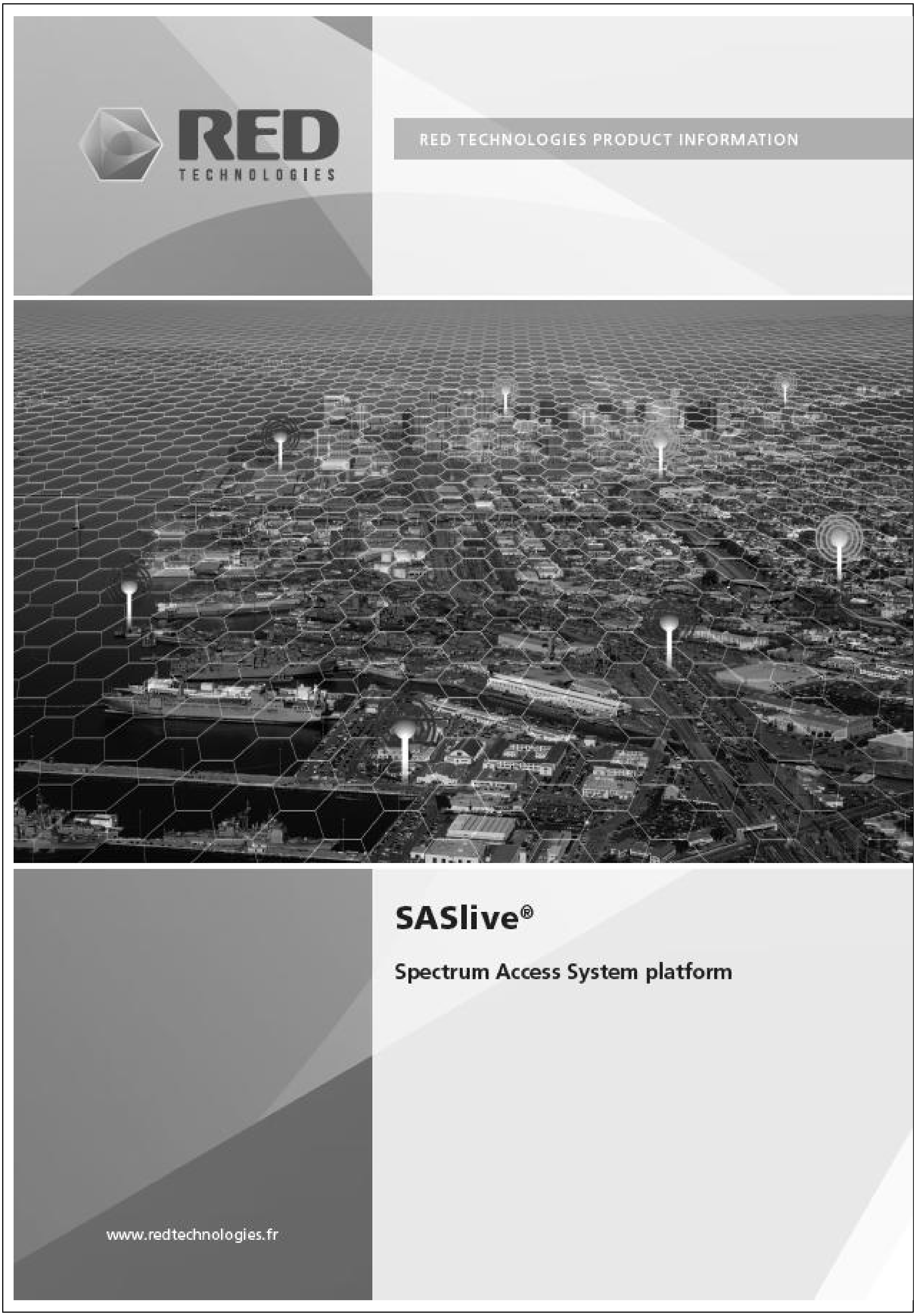
LSA Simulator® key features

- With **LSA Simulator®** we localize and quantify available LSA spectrum under our clients' national specific policy and constraints.
- Data extracted from **LSA Simulator®** is analyzed by our experts to quantitatively and qualitatively evaluate LSA opportunities.
- Using **LSA Simulator®** we generate the relevant incumbent's protection criteria that can be subsequently used to update our **LSAlive Repository®**.

RED Technologies SAS
130, rue de Lourmel,
75015 Paris, France

Tel: + 33 1 84 16 88 32
Web: www.redtechnologies.fr
SIRET: 752 992 735 R.C.S. Paris

6.3.2. SASlive© Marketing Brochure



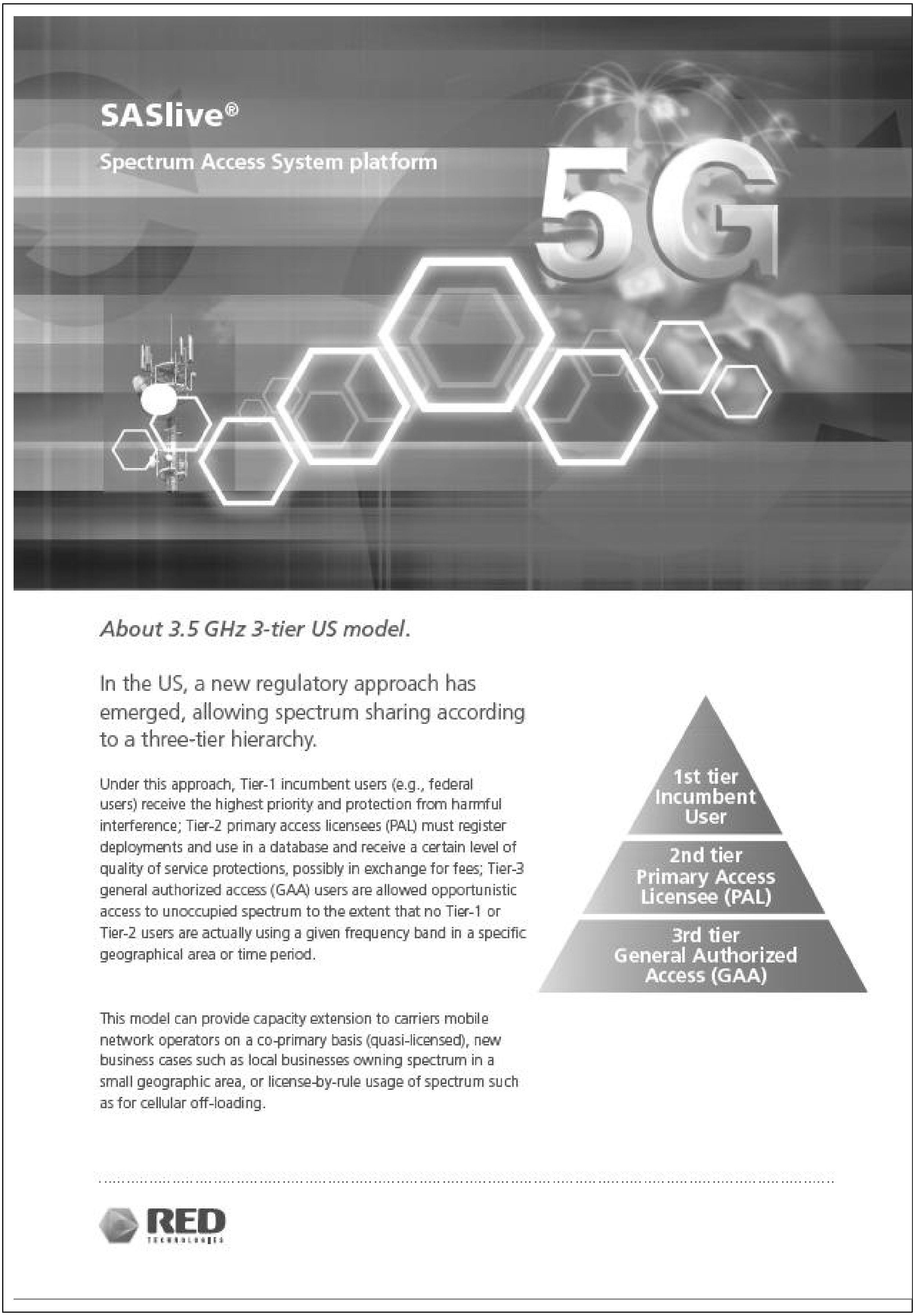
RED TECHNOLOGIES

RED TECHNOLOGIES PRODUCT INFORMATION

SASlive®

Spectrum Access System platform

www.redtechnologies.fr



SASlive®

Spectrum Access System platform

About 3.5 GHz 3-tier US model.

In the US, a new regulatory approach has emerged, allowing spectrum sharing according to a three-tier hierarchy.

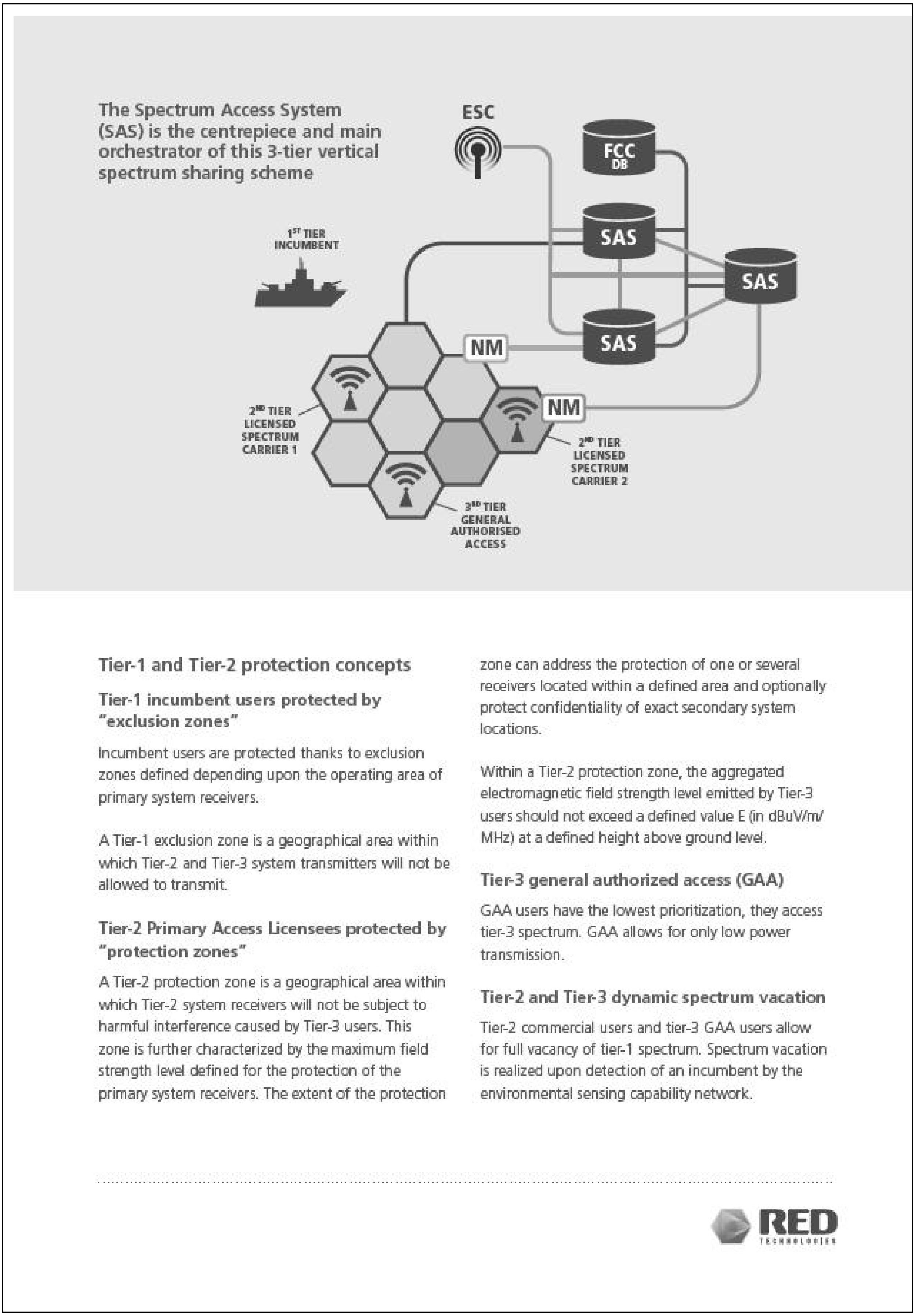
Under this approach, Tier-1 incumbent users (e.g., federal users) receive the highest priority and protection from harmful interference; Tier-2 primary access licensees (PAL) must register deployments and use in a database and receive a certain level of quality of service protections, possibly in exchange for fees; Tier-3 general authorized access (GAA) users are allowed opportunistic access to unoccupied spectrum to the extent that no Tier-1 or Tier-2 users are actually using a given frequency band in a specific geographical area or time period.

1st tier
Incumbent
User

2nd tier
Primary Access
Licensee (PAL)

3rd tier
General Authorized
Access (GAA)

This model can provide capacity extension to carriers mobile network operators on a co-primary basis (quasi-licensed), new business cases such as local businesses owning spectrum in a small geographic area, or license-by-rule usage of spectrum such as for cellular off-loading.



The Spectrum Access System (SAS) is the centrepiece and main orchestrator of this 3-tier vertical spectrum sharing scheme

ESC
FCC DB
SAS
SAS
SAS
1ST TIER INCUMBENT
NM
NM
2ND TIER LICENSED SPECTRUM CARRIER 1
2ND TIER LICENSED SPECTRUM CARRIER 2
3RD TIER GENERAL AUTHORISED ACCESS

Tier-1 and Tier-2 protection concepts

Tier-1 incumbent users protected by "exclusion zones"

Incumbent users are protected thanks to exclusion zones defined depending upon the operating area of primary system receivers.

A Tier-1 exclusion zone is a geographical area within which Tier-2 and Tier-3 system transmitters will not be allowed to transmit.

Tier-2 Primary Access Licensees protected by "protection zones"

A Tier-2 protection zone is a geographical area within which Tier-2 system receivers will not be subject to harmful interference caused by Tier-3 users. This zone is further characterized by the maximum field strength level defined for the protection of the primary system receivers. The extent of the protection zone can address the protection of one or several receivers located within a defined area and optionally protect confidentiality of exact secondary system locations.

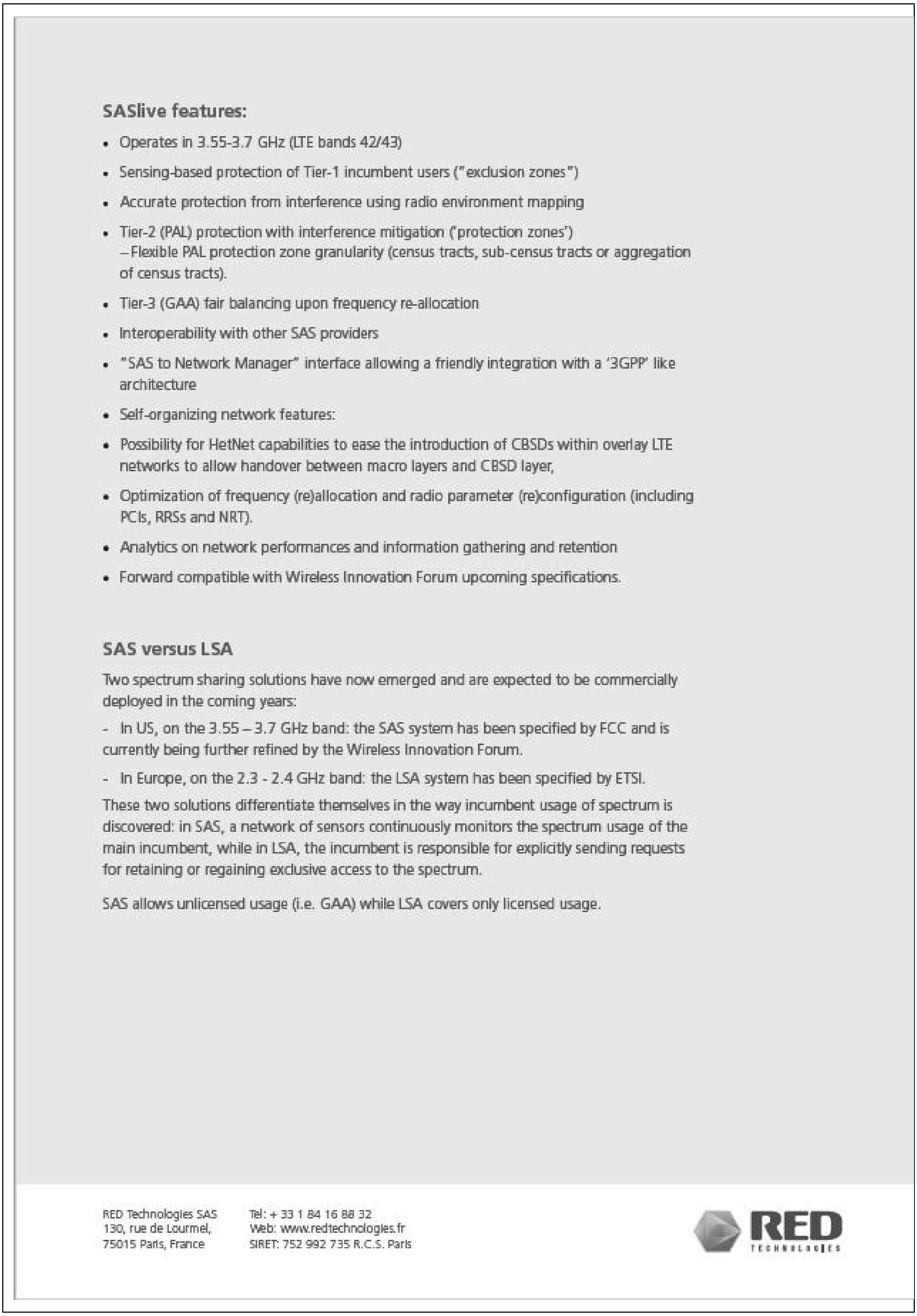
Within a Tier-2 protection zone, the aggregated electromagnetic field strength level emitted by Tier-3 users should not exceed a defined value E (in dBuV/m/MHz) at a defined height above ground level.

Tier-3 general authorized access (GAA)

GAA users have the lowest prioritization, they access tier-3 spectrum. GAA allows for only low power transmission.

Tier-2 and Tier-3 dynamic spectrum vacation

Tier-2 commercial users and tier-3 GAA users allow for full vacancy of tier-1 spectrum. Spectrum vacation is realized upon detection of an incumbent by the environmental sensing capability network.



SASlive features:

- Operates in 3.55-3.7 GHz (LTE bands 42/43)
- Sensing-based protection of Tier-1 incumbent users ("exclusion zones")
- Accurate protection from interference using radio environment mapping
- Tier-2 (PAL) protection with interference mitigation ('protection zones')
  – Flexible PAL protection zone granularity (census tracts, sub-census tracts or aggregation of census tracts).
- Tier-3 (GAA) fair balancing upon frequency re-allocation
- Interoperability with other SAS providers
- "SAS to Network Manager" interface allowing a friendly integration with a '3GPP' like architecture
- Self-organizing network features:
- Possibility for HetNet capabilities to ease the introduction of CBSDs within overlay LTE networks to allow handover between macro layers and CBSD layer,
- Optimization of frequency (re)allocation and radio parameter (re)configuration (including PCIs, RRSs and NRT).
- Analytics on network performances and information gathering and retention
- Forward compatible with Wireless Innovation Forum upcoming specifications.

SAS versus LSA

Two spectrum sharing solutions have now emerged and are expected to be commercially deployed in the coming years:

- In US, on the 3.55 – 3.7 GHz band: the SAS system has been specified by FCC and is currently being further refined by the Wireless Innovation Forum.
- In Europe, on the 2.3 - 2.4 GHz band: the LSA system has been specified by ETSI.

These two solutions differentiate themselves in the way incumbent usage of spectrum is discovered: in SAS, a network of sensors continuously monitors the spectrum usage of the main incumbent, while in LSA, the incumbent is responsible for explicitly sending requests for retaining or regaining exclusive access to the spectrum.

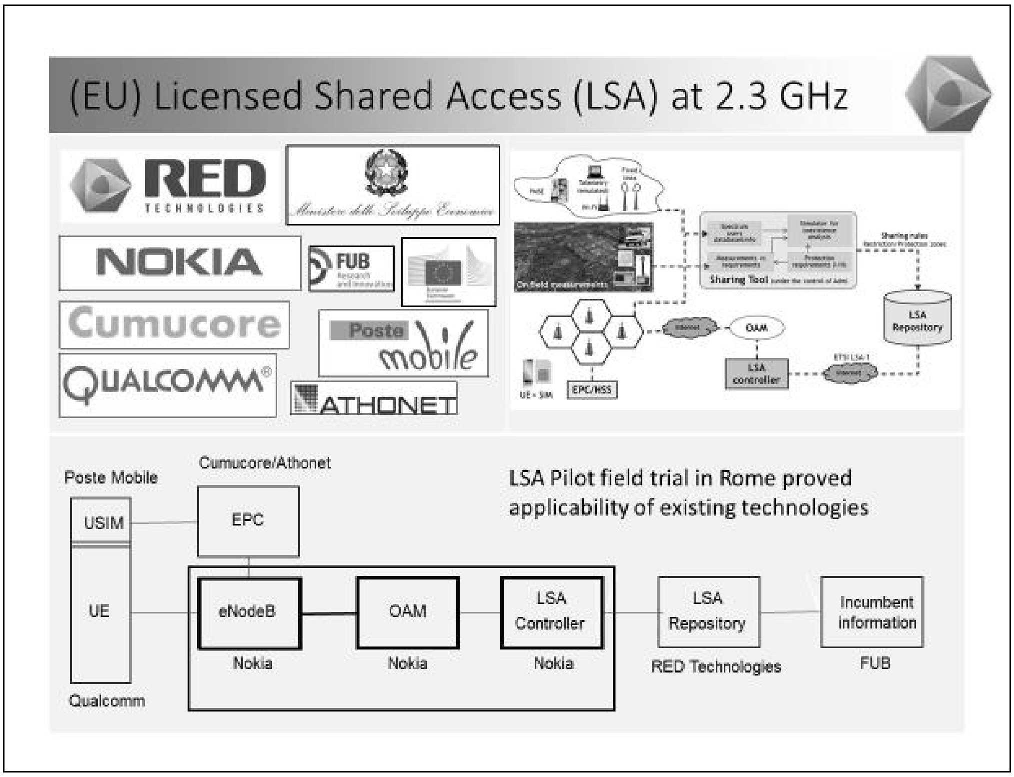
SAS allows unlicensed usage (i.e. GAA) while LSA covers only licensed usage.

RED Technologies SAS
130, rue de Lourmel,
75015 Paris, France

Tel: + 33 1 84 16 88 32
Web: www.redtechnologies.fr
SIRET: 752 992 735 R.C.S. Paris

6.3.3. 2.3 GHz LSA Pilot

6.3.3.1. 2.3 GHz LSA Pilot, Rome, Italy

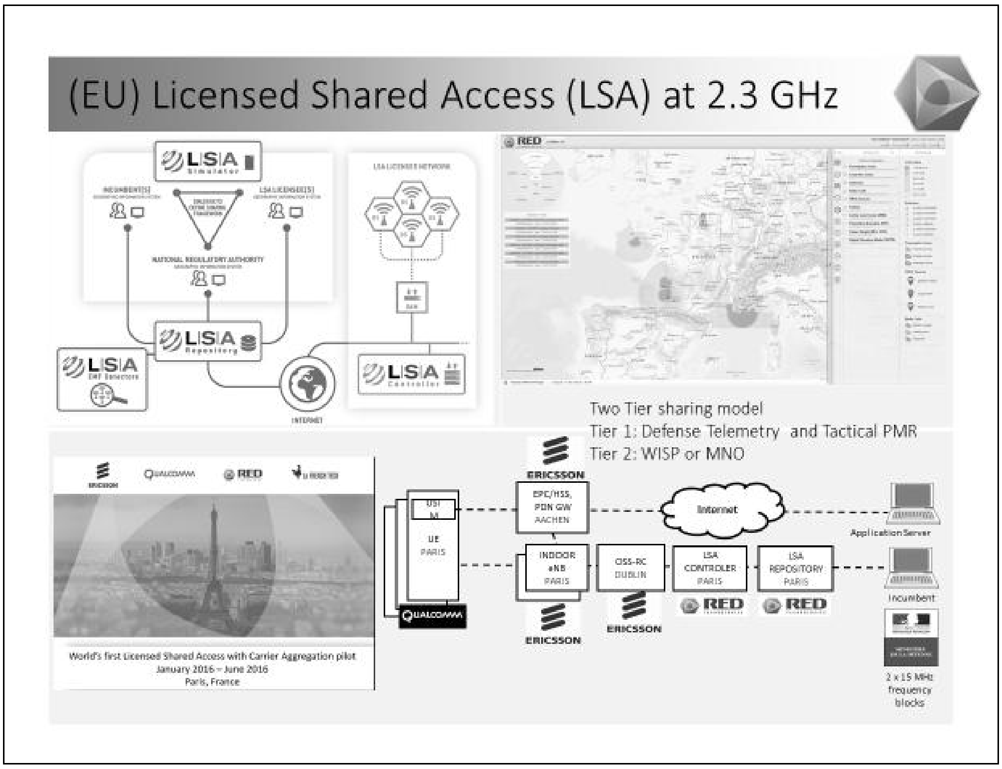


(EU) Licensed Shared Access (LSA) at 2.3 GHz

LSA Pilot field trial in Rome proved applicability of existing technologies

Figure 28: 2.3 GHz LSA Pilot, Rome, Italy

6.3.3.2. 2.3 GHz LSA Pilot, Paris, France



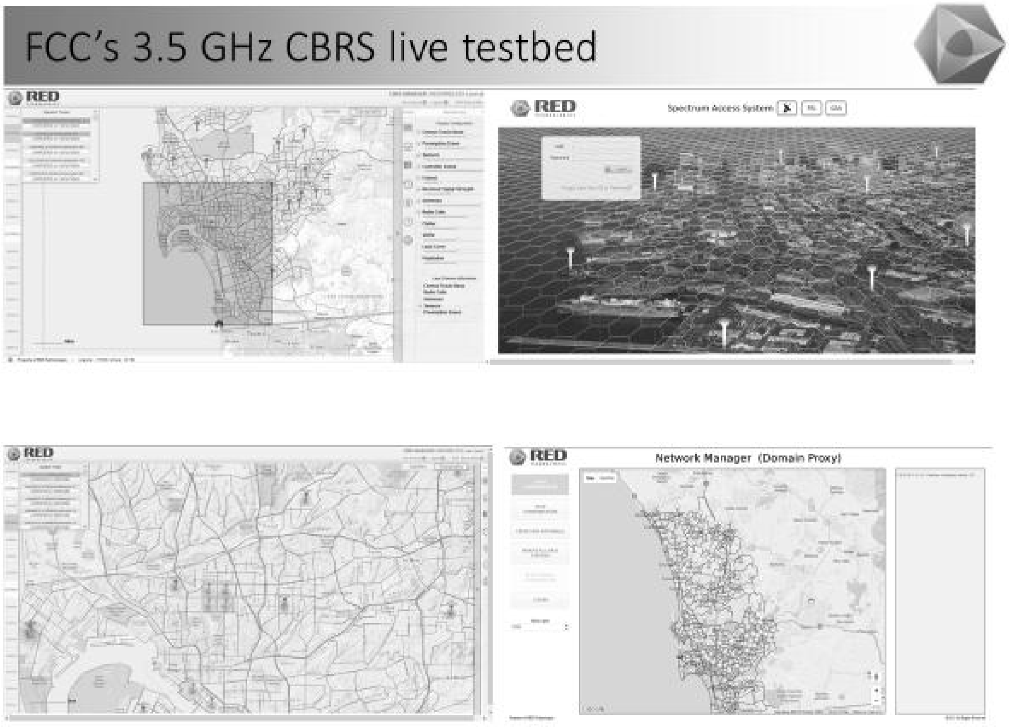
(EU) Licensed Shared Access (LSA) at 2.3 GHz

Two Tier sharing model
Tier 1: Defense Telemetry and Tactical PMR
Tier 2: WISP or MNO

World's first Licensed Shared Access with Carrier Aggregation pilot
January 2016 – June 2016
Paris, France

Figure 29: 2.3 GHz LSA Pilot, Paris, France

6.3.4. 3.5 GHz CBRS band testbed, Rennes, France

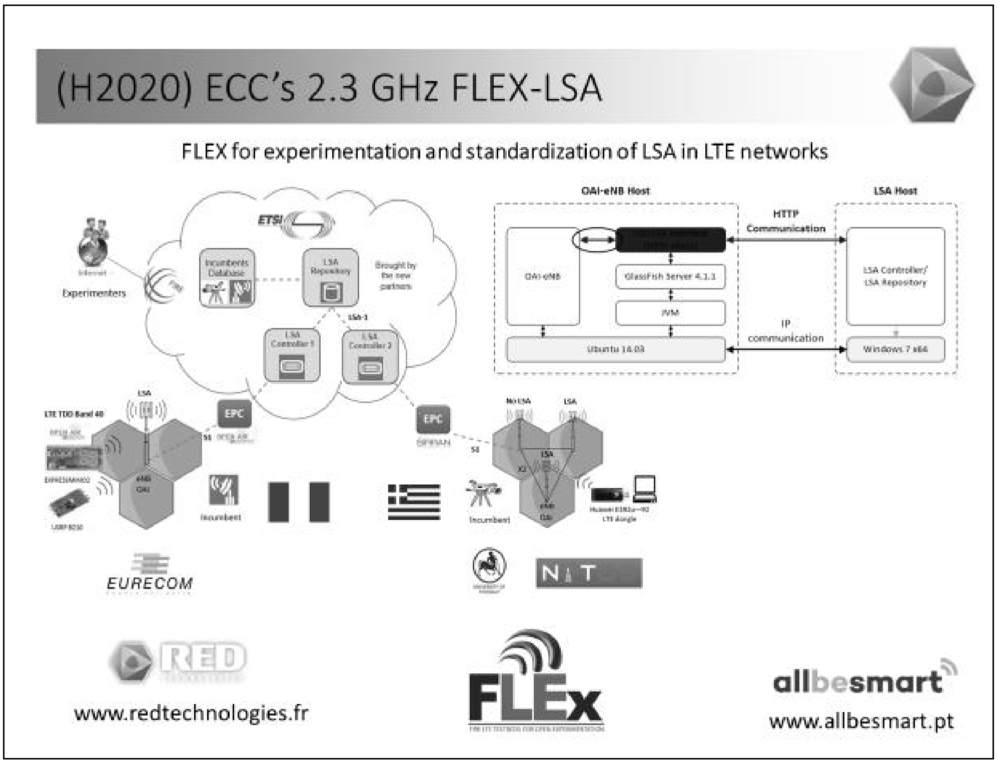


FCC's 3.5 GHz CBRS live testbed

Figure 30: 3.5 GHz CBRS band testbed, Rennes, France

6.3.5. Company's European Research Projects on Spectrum Sharing

6.3.5.1. H2020 2.3 GHz FLEX LSA

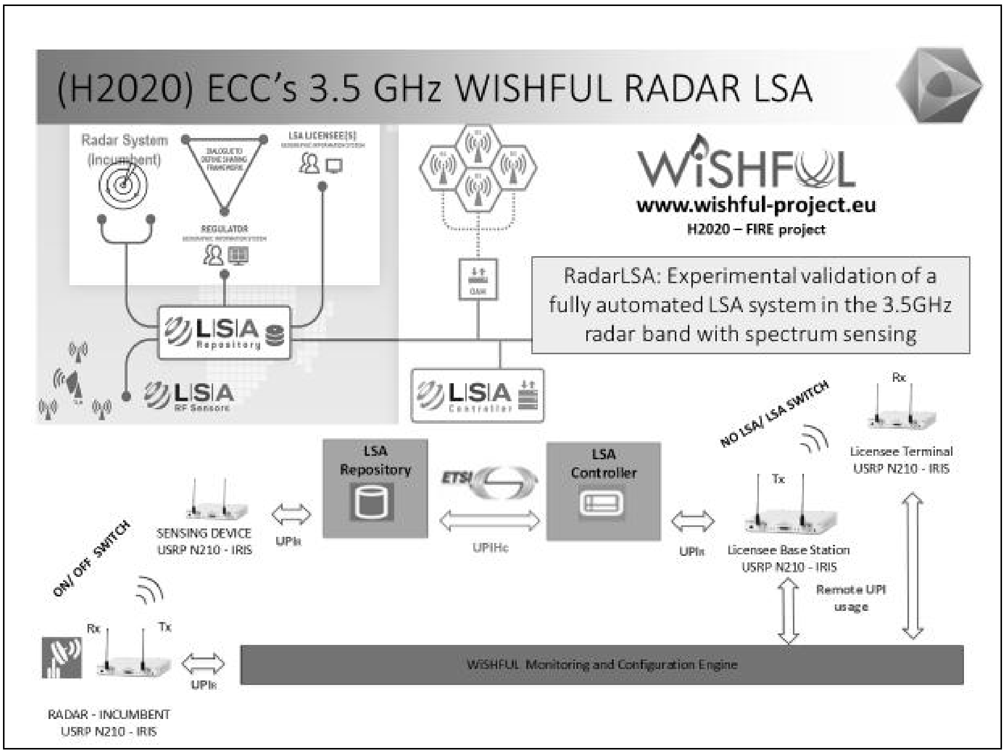


(H2020) ECC's 2.3 GHz FLEX-LSA

FLEX for experimentation and standardization of LSA in LTE networks

Figure 31: H2020 2.3 GHz FLEX LSA

6.3.5.2. H2020 3.5 GHz WISHFUL RADAR LSA



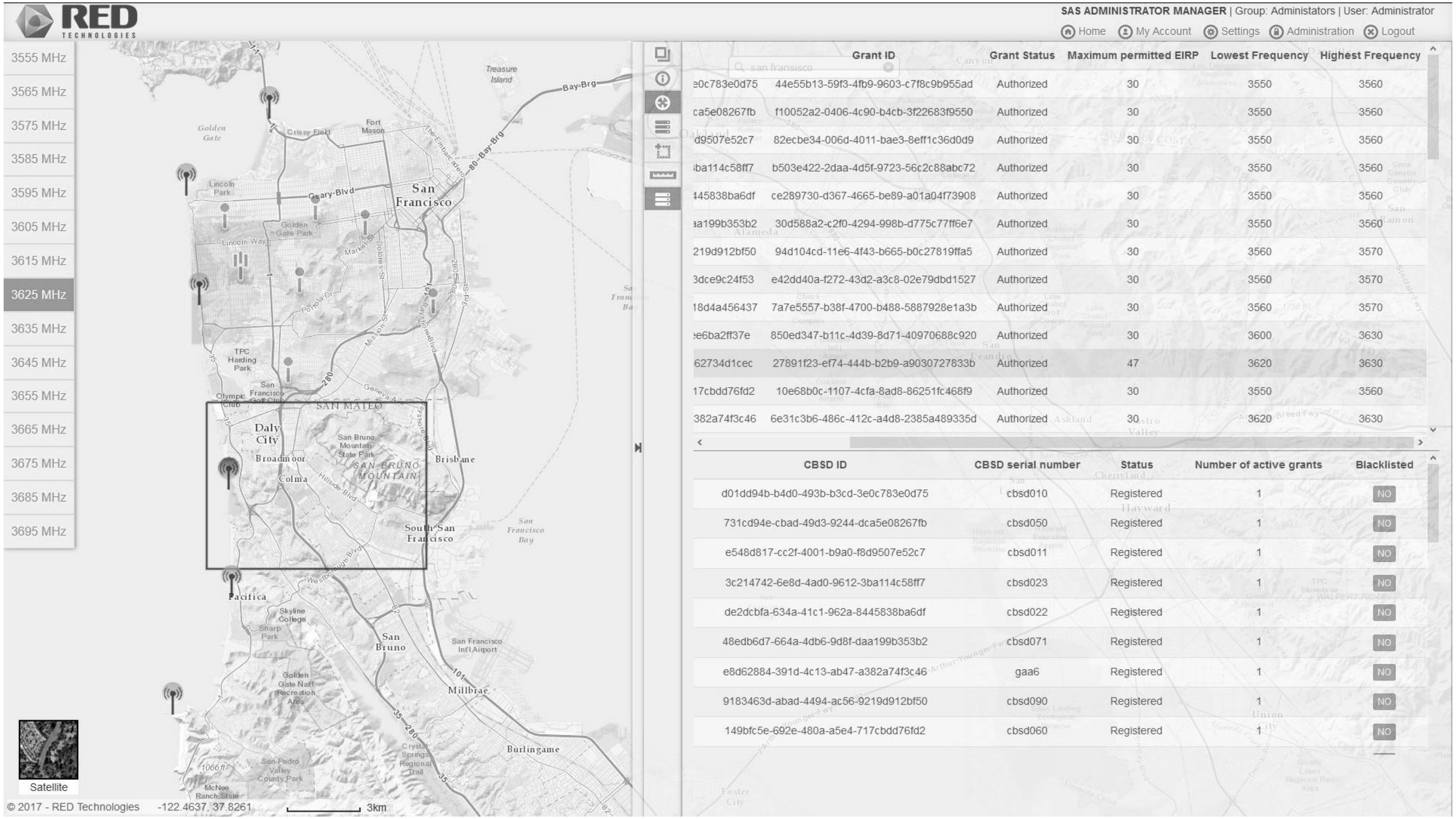
(H2020) ECC's 3.5 GHz WISHFUL RADAR LSA

RadarLSA: Experimental validation of a fully automated LSA system in the 3.5GHz radar band with spectrum sensing

Figure 32: H2020 3.5 WISHFUL GHz RADAR LSA

6.4. SASlive© GUI

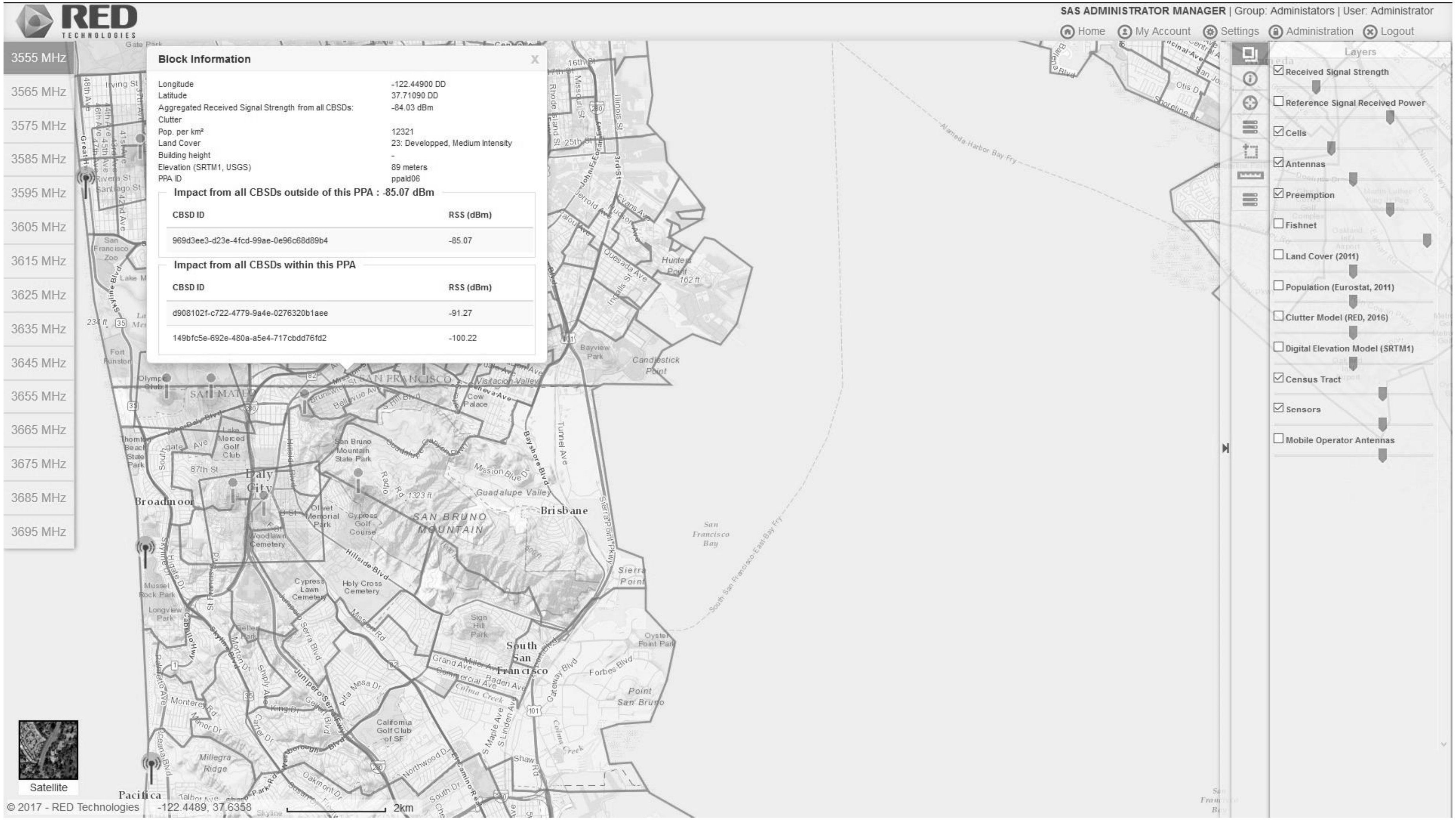
This section shows some screen shots of Graphical User Interface of the SASlive©.



	Grant ID	Grant Status	Maximum permitted EIRP	Lowest Frequency	Highest Frequency
ɜ0c783e0d75	44e55b13-59f3-4fb9-9603-c7f8c9b955ad	Authorized	30	3550	3560
ca5e08267fb	f10052a2-0406-4c90-b4cb-3f22683f9550	Authorized	30	3550	3560
d9507e52c7	82ecbe34-006d-4011-bae3-8eff1c36d0d9	Authorized	30	3550	3560
ba114c58ff7	b503e422-2daa-4d5f-9723-56c2c88abc72	Authorized	30	3550	3560
445838ba6df	ce289730-d367-4665-be89-a01a04f73908	Authorized	30	3550	3560
aa199b353b2	30d588a2-c2f0-4294-998b-d775c77ff6e7	Authorized	30	3550	3560
219d912bf50	94d104cd-11e6-4f43-b665-b0c27819ffa5	Authorized	30	3560	3570
3dce9c24f53	e42dd40a-f272-43d2-a3c8-02e79dbd1527	Authorized	30	3560	3570
18d4a456437	7a7e5557-b38f-4700-b488-5887928e1a3b	Authorized	30	3560	3570
ee6ba2ff37e	850ed347-b11c-4d39-8d71-40970688c920	Authorized	30	3600	3630
62734d1cec	27891f23-ef74-444b-b2b9-a9030727833b	Authorized	47	3620	3630
17cbdd76fd2	10e68b0c-1107-4cfa-8ad8-86251fc468f9	Authorized	30	3550	3560
382a74f3c46	6e31c3b6-486c-412c-a4d8-2385a489335d	Authorized	30	3620	3630

CBSD ID	CBSD serial number	Status	Number of active grants	Blacklisted
d01dd94b-b4d0-493b-b3cd-3e0c783e0d75	cbsd010	Registered	1	NO
731cd94e-cbad-49d3-9244-dca5e08267fb	cbsd050	Registered	1	NO
e548d817-cc2f-4001-b9a0-f8d9507e52c7	cbsd011	Registered	1	NO
3c214742-6e8d-4ad0-9612-3ba114c58ff7	cbsd023	Registered	1	NO
de2dcbfa-634a-41c1-962a-8445838ba6df	cbsd022	Registered	1	NO
48edb6d7-664a-4db6-9d8f-daa199b353b2	cbsd071	Registered	1	NO
e8d62884-391d-4c13-ab47-a382a74f3c46	gaa6	Registered	1	NO
9183463d-abad-4494-ac56-9219d912bf50	cbsd090	Registered	1	NO
149bfc5e-692e-480a-a5e4-717cbdd76fd2	cbsd060	Registered	1	NO

Figure 33: Exclusion zone / List of grants / List of registered CBSDs



Block Information

Longitude	-122.44900 DD
Latitude	37.71090 DD
Aggregated Received Signal Strength from all CBSDs:	-84.03 dBm
Clutter	
Pop. per km²	12321
Land Cover	23: Developped, Medium Intensity
Building height	-
Elevation (SRTM1, USGS)	89 meters
PPA ID	ppald06

Impact from all CBSDs outside of this PPA : -85.07 dBm

CBSD ID	RSS (dBm)
969d3ee3-d23e-4fcd-99ae-0e96c68d89b4	-85.07

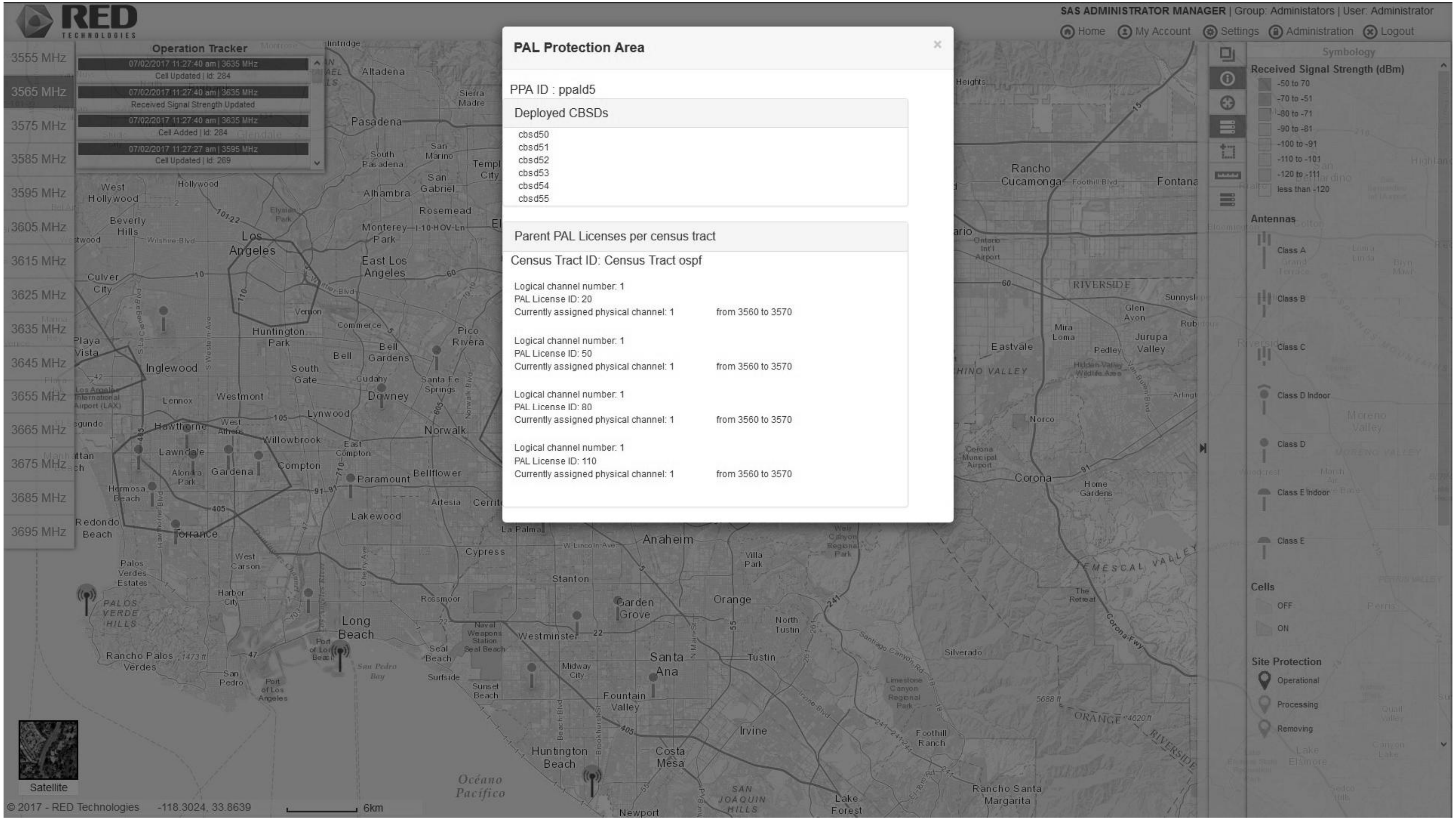
Impact from all CBSDs within this PPA

CBSD ID	RSS (dBm)
d908102f-c722-4779-9a4e-0276320b1aee	-91.27
149bfc5e-692e-480a-a5e4-717cbdd76fd2	-100.22

Layers

☑ Received Signal Strength
□ Reference Signal Received Power
☑ Cells
☑ Antennas
☑ Preemption
□ Fishnet
□ Land Cover (2011)
□ Population (Eurostat, 2011)
□ Clutter Model (RED, 2016)
□ Digital Elevation Model (SRTM1)
☑ Census Tract
☑ Sensors
□ Mobile Operator Antennas

Figure 34: Received Signal Strength within a PPA



Operation Tracker

07/02/2017 11:27:40 am | 3635 MHz
Cell Updated | Id: 284

07/02/2017 11:27:40 am | 3635 MHz
Received Signal Strength Updated

07/02/2017 11:27:40 am | 3635 MHz
Cell Added | Id: 284

07/02/2017 11:27:27 am | 3595 MHz
Cell Updated | Id: 269

PAL Protection Area ×

PPA ID : ppald5

Deployed CBSDs

cbsd50
cbsd51
cbsd52
cbsd53
cbsd54
cbsd55

Parent PAL Licenses per census tract

Census Tract ID: Census Tract ospf

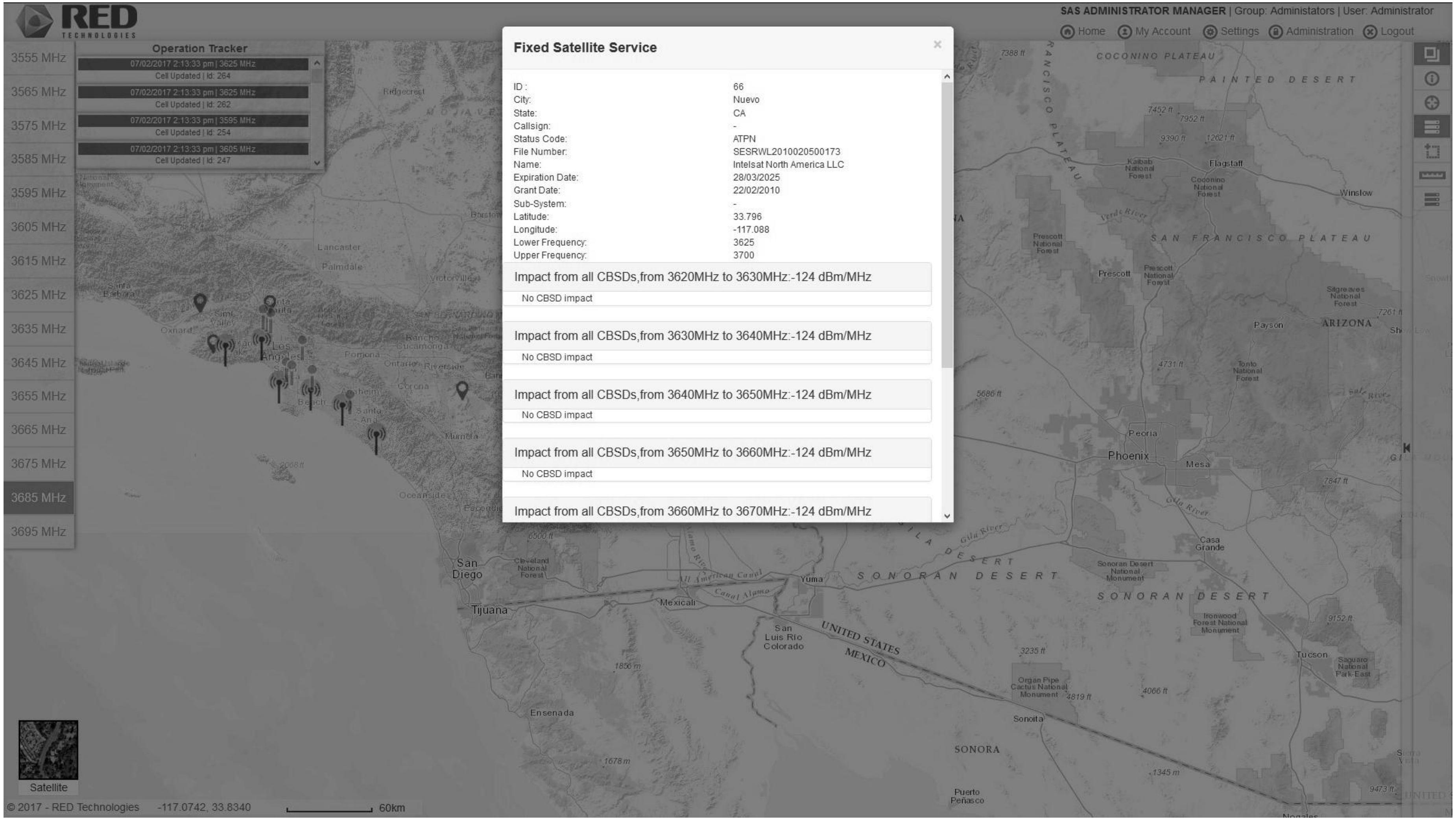
Logical channel number: 1
PAL License ID: 20
Currently assigned physical channel: 1 from 3560 to 3570

Logical channel number: 1
PAL License ID: 50
Currently assigned physical channel: 1 from 3560 to 3570

Logical channel number: 1
PAL License ID: 80
Currently assigned physical channel: 1 from 3560 to 3570

Logical channel number: 1
PAL License ID: 110
Currently assigned physical channel: 1 from 3560 to 3570

Figure 35: PPA Information



Operation Tracker

07/02/2017 2:13:33 pm | 3625 MHz
Cell Updated | Id: 264

07/02/2017 2:13:33 pm | 3625 MHz
Cell Updated | Id: 262

07/02/2017 2:13:33 pm | 3595 MHz
Cell Updated | Id: 254

07/02/2017 2:13:33 pm | 3605 MHz
Cell Updated | Id: 247

Fixed Satellite Service

ID :	66
City:	Nuevo
State:	CA
Callsign:	-
Status Code:	ATPN
File Number:	SESRWL2010020500173
Name:	Intelsat North America LLC
Expiration Date:	28/03/2025
Grant Date:	22/02/2010
Sub-System:	-
Latitude:	33.796
Longitude:	-117.088
Lower Frequency:	3625
Upper Frequency:	3700

Impact from all CBSDs,from 3620MHz to 3630MHz:-124 dBm/MHz

No CBSD impact

Impact from all CBSDs,from 3630MHz to 3640MHz:-124 dBm/MHz

No CBSD impact

Impact from all CBSDs,from 3640MHz to 3650MHz:-124 dBm/MHz

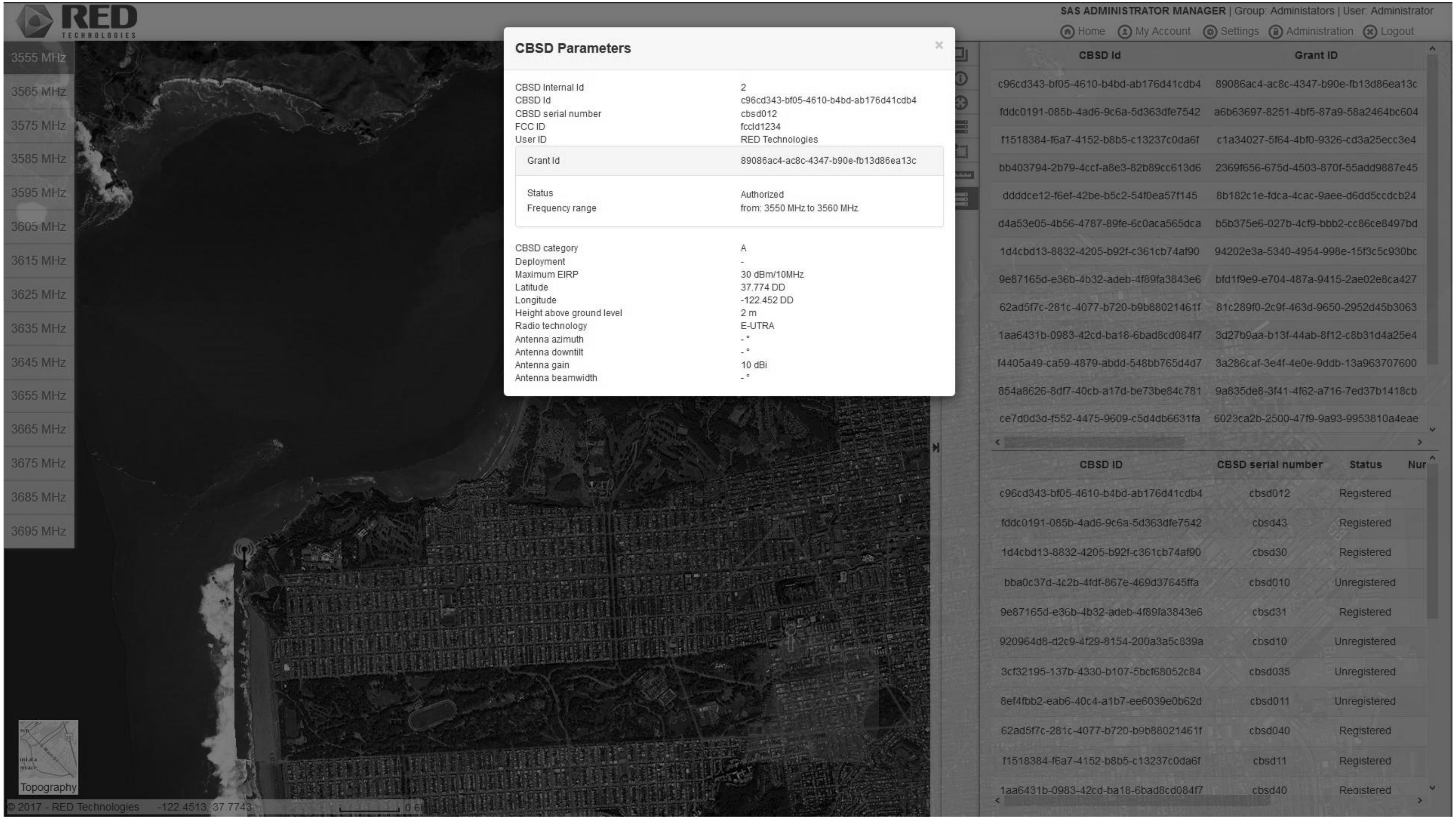
No CBSD impact

Impact from all CBSDs,from 3650MHz to 3660MHz:-124 dBm/MHz

No CBSD impact

Impact from all CBSDs,from 3660MHz to 3670MHz:-124 dBm/MHz

Figure 36: Fixed Satellite Service information



CBSD Parameters ×

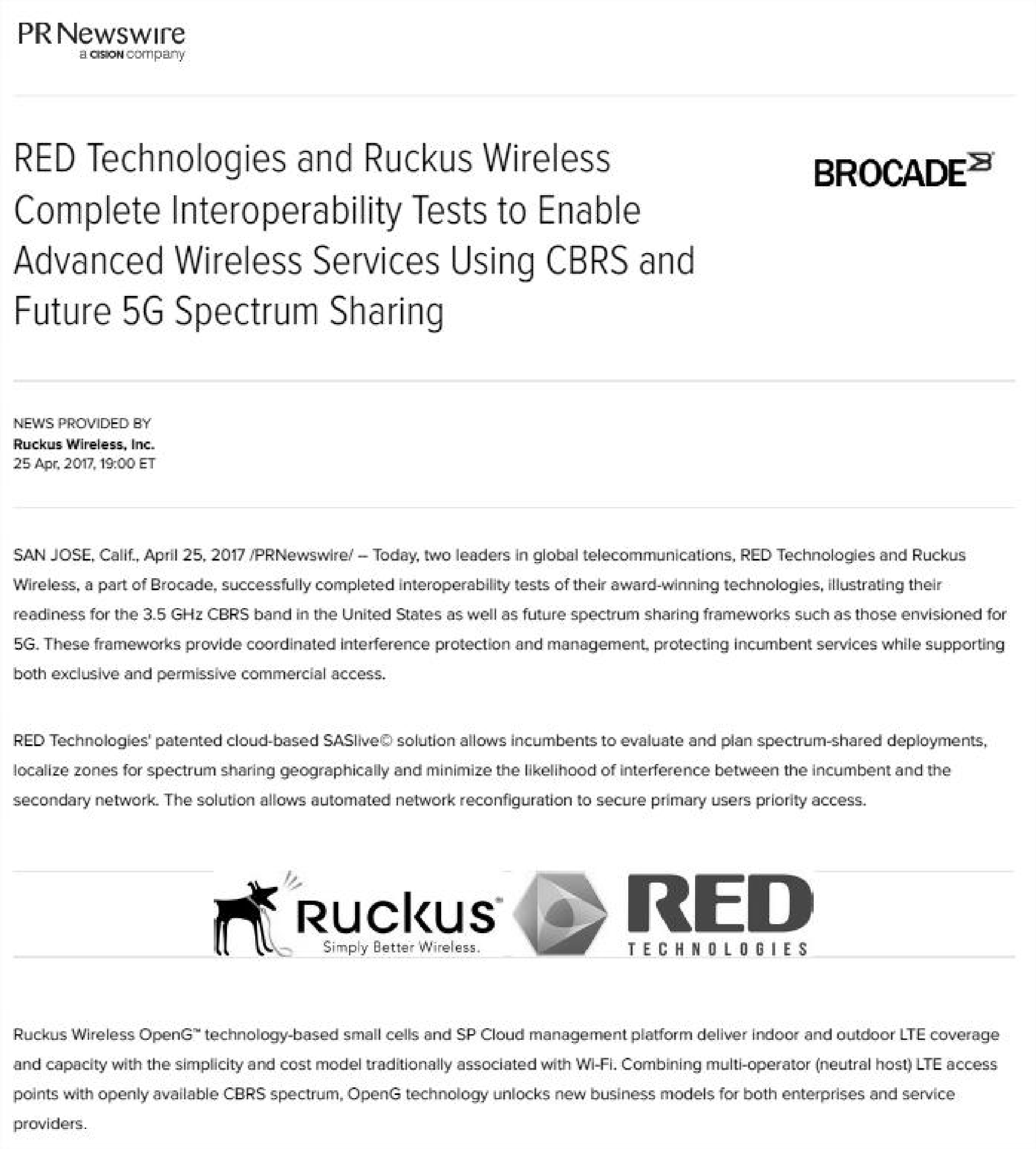
CBSD Internal Id	2
CBSD Id	c96cd343-bf05-4610-b4bd-ab176d41cdb4
CBSD serial number	cbsd012
FCC ID	fccld1234
User ID	RED Technologies
Grant Id	89086ac4-ac8c-4347-b90e-fb13d86ea13c
Status	Authorized
Frequency range	from: 3550 MHz to 3560 MHz
CBSD category	A
Deployment	-
Maximum EIRP	30 dBm/10MHz
Latitude	37.774 DD
Longitude	-122.452 DD
Height above ground level	2 m
Radio technology	E-UTRA
Antenna azimuth	- °
Antenna downtilt	- °
Antenna gain	10 dBi
Antenna beamwidth	- °

CBSD Id	Grant ID
c96cd343-bf05-4610-b4bd-ab176d41cdb4	89086ac4-ac8c-4347-b90e-fb13d86ea13c
fddc0191-085b-4ad6-9c6a-5d363dfe7542	a6b63697-8251-4bf5-87a9-58a2464bc604
f1518384-f6a7-4152-b8b5-c13237c0da6f	c1a34027-5f64-4bf0-9326-cd3a25ecc3e4
bb403794-2b79-4ccf-a8e3-82b89cc613d6	2369f656-675d-4503-870f-55add9887e45
ddddce12-f6ef-42be-b5c2-54f0ea57f145	8b182c1e-fdca-4cac-9aee-d6dd5ccdcb24
d4a53e05-4b56-4787-89fe-6c0aca565dca	b5b375e6-027b-4cf9-bbb2-cc86ce8497bd
1d4cbd13-8832-4205-b92f-c361cb74af90	94202e3a-5340-4954-998e-15f3c5c930bc
9e87165d-e36b-4b32-adeb-4f89fa3843e6	bfd1f9e9-e704-487a-9415-2ae02e8ca427
62ad5f7c-281c-4077-b720-b9b88021461f	81c289f0-2c9f-463d-9650-2952d45b3063
1aa6431b-0983-42cd-ba18-6bad8cd084f7	3d27b9aa-b13f-44ab-8f12-c8b31d4a25e4
f4405a49-ca59-4879-abdd-548bb765d4d7	3a286caf-3e4f-4e0e-9ddb-13a963707600
854a8626-8df7-40cb-a17d-be73be84c781	9a835de8-3f41-4f62-a716-7ed37b1418cb
ce7d0d3d-f552-4475-9609-c5d4db6631fa	6023ca2b-2500-47f9-9a93-9953810a4eae

CBSD ID	CBSD serial number	Status	Nur
c96cd343-bf05-4610-b4bd-ab176d41cdb4	cbsd012	Registered	
fddc0191-085b-4ad6-9c6a-5d363dfe7542	cbsd43	Registered	
1d4cbd13-8832-4205-b92f-c361cb74af90	cbsd30	Registered	
bba0c37d-4c2b-4fdf-867e-469d37645ffa	cbsd010	Unregistered	
9e87165d-e36b-4b32-adeb-4f89fa3843e6	cbsd31	Registered	
920964d8-d2c9-4f29-8154-200a3a5c839a	cbsd10	Unregistered	
3cf32195-137b-4330-b107-5bcf68052c84	cbsd035	Unregistered	
8ef4fbb2-eab6-40c4-a1b7-ee6039e0b62d	cbsd011	Unregistered	
62ad5f7c-281c-4077-b720-b9b88021461f	cbsd040	Registered	
f1518384-f6a7-4152-b8b5-c13237c0da6f	cbsd11	Registered	
1aa6431b-0983-42cd-ba18-6bad8cd084f7	cbsd40	Registered	

Figure 37: CBSD Information

6.5. PRESS RELEASE



PR Newswire
a CISION company

RED Technologies and Ruckus Wireless Complete Interoperability Tests to Enable Advanced Wireless Services Using CBRS and Future 5G Spectrum Sharing

BROCADE

NEWS PROVIDED BY
Ruckus Wireless, Inc.
25 Apr, 2017, 19:00 ET

SAN JOSE, Calif., April 25, 2017 /PRNewswire/ -- Today, two leaders in global telecommunications, RED Technologies and Ruckus Wireless, a part of Brocade, successfully completed interoperability tests of their award-winning technologies, illustrating their readiness for the 3.5 GHz CBRS band in the United States as well as future spectrum sharing frameworks such as those envisioned for 5G. These frameworks provide coordinated interference protection and management, protecting incumbent services while supporting both exclusive and permissive commercial access.

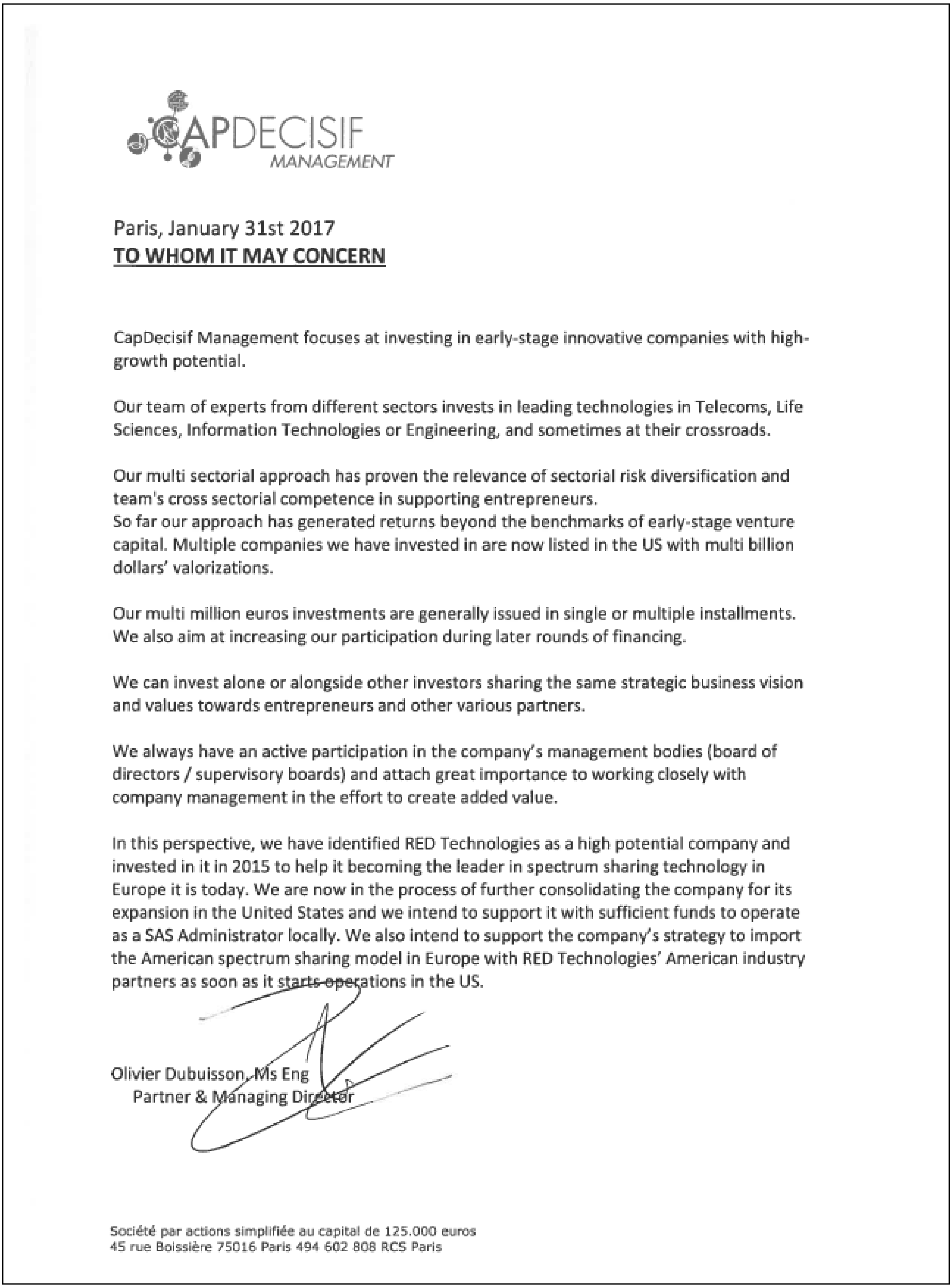
RED Technologies' patented cloud-based SASlive© solution allows incumbents to evaluate and plan spectrum-shared deployments, localize zones for spectrum sharing geographically and minimize the likelihood of interference between the incumbent and the secondary network. The solution allows automated network reconfiguration to secure primary users priority access.

Ruckus Wireless OpenG™ technology-based small cells and SP Cloud management platform deliver indoor and outdoor LTE coverage and capacity with the simplicity and cost model traditionally associated with Wi-Fi. Combining multi-operator (neutral host) LTE access points with openly available CBRS spectrum, OpenG technology unlocks new business models for both enterprises and service providers.

Figure 38: Press release

Full article: http://www.prnewswire.com/news-releases/red-technologies-and-ruckus-wireless-complete-interoperability-tests-to-enable-advanced-wireless-services-using-cbrs-and-future-5g-spectrum-sharing-300445611.html

6.6. SUPPORT LETTER FROM CAP DÉCISIF



CAPDECISIF
MANAGEMENT

Paris, January 31st 2017

TO WHOM IT MAY CONCERN

CapDecisif Management focuses at investing in early-stage innovative companies with high-growth potential.

Our team of experts from different sectors invests in leading technologies in Telecoms, Life Sciences, Information Technologies or Engineering, and sometimes at their crossroads.

Our multi sectorial approach has proven the relevance of sectorial risk diversification and team's cross sectorial competence in supporting entrepreneurs.
So far our approach has generated returns beyond the benchmarks of early-stage venture capital. Multiple companies we have invested in are now listed in the US with multi billion dollars' valorizations.

Our multi million euros investments are generally issued in single or multiple installments. We also aim at increasing our participation during later rounds of financing.

We can invest alone or alongside other investors sharing the same strategic business vision and values towards entrepreneurs and other various partners.

We always have an active participation in the company's management bodies (board of directors / supervisory boards) and attach great importance to working closely with company management in the effort to create added value.

In this perspective, we have identified RED Technologies as a high potential company and invested in it in 2015 to help it becoming the leader in spectrum sharing technology in Europe it is today. We are now in the process of further consolidating the company for its expansion in the United States and we intend to support it with sufficient funds to operate as a SAS Administrator locally. We also intend to support the company's strategy to import the American spectrum sharing model in Europe with RED Technologies' American industry partners as soon as it starts operations in the US.

Olivier Dubuisson, Ms Eng
Partner & Managing Director

Société par actions simplifiée au capital de 125.000 euros
45 rue Boissière 75016 Paris 494 602 808 RCS Paris

Figure 39: Support letter from Cap Décisif

END OF DOCUMENT